SecurityCenter 4.6 Administration Guide

April 11, 2013

(Revision 5)

Table of Contents

Introduction 5
Standards and Conventions 5
Abbreviations 6
SecurityCenter Administrator Functions 6
Starting/Halting SecurityCenter 6
SecurityCenter Home Page/Dashboard 7
System Configuration 9
Configuration 9
Basic 9
Mail 10
LDAP 11
Expiration 13
Update 14
Authentication 14
Reporting/Scanning 16
Miscellaneous 17
Diagnostics 18
Preferences 19
Basic 19
Notifications 19
Keys 20
Remote LCE Key Exchange 21
Publishing Sites 21
SSL Client Certificate Authentication 23
Configure SecurityCenter for Certificates 23
Connect with SSL Certificate Enabled Browser 24
CoSign Configuration Instructions 26
Resource Management 27
Nessus Scanners 27
Adding a Nessus Scanner 28
Configure SecurityCenter for Custom Certificates to Verify Hostname 29
Nessus Perimeter Service Scanners 30
Nessus Scanner Details 32
Scan Zones 32
Passive Vulnerability Scanners 33
Log Correlation Engines 35
Log Correlation Engine Clients 37
Data Management 40
Repositories 40
Local Repository 41
Remote Repository 42
Offline Repository 44
Accept Risk Rules 46
Recast Risk Rules 47

User Management 48
Organizations 48
Support 55
Audit Files 55
Credentials 56
Scan Policies 57
Add a Scan Policy 58
Basic 58
Audit Files 61
Plugins 62
Preferences 63
Users 78
Administrators 79
Roles 80
User Access Control 81
Status 83
Job Queue 83
Logs 84
Audit Admin & User Activity 84
Startup and Shutdown of the Audit Functions 84
Accessing the Audit Records 85
Modification to the Audit Configuration and Administrator Log 87
Audit Log Data Selection 87
Plugins 87
Update Plugins 88
Upload Plugins 88
Other Plugin Options 89
Troubleshooting 89
SecurityCenter 89
SecurityCenter does not appear to be operational 89
Forgot login credentials 90
Invalid license error 90
Reporting does not work 90
LCE 90
LCE server does not appear to be operational: 90
No events from an attached LCE server 90
Invalid LCE license 91
Nessus 91
Nessus server does not appear to be operational: 91
Cannot add a Nessus server 91
Nessus scans fail to complete 91
Nessus plugins fail to update 92
PVS 92
PVS server does not appear to be operational 92
Can't add a PVS server 92
No vulnerabilities are being received from the PVS server 92
PVS plugins fail to update 92
Appendix 1: Non-Tenable License Declarations 94
Related Third-Party and Open-Source Licenses 94
Tenable Third-Party Licensed Software 95

ChartDirector Version 5.0 95
Nessus Plugins 96
Appendix 2: Manual LCE Key Exchange 97
Appendix 3: Nessus SSL Configuration 98
Introduction 98
Overview of SSL Certificates and Keys 98
Certificate Authority 98
Nessus Server 98
Nessus Client 98
Nessus Configuration for Unix 98
Commands and Relevant Files 98
Certificate Authority and Nessus Server Certificate 98
Nessus Client Keys 99
Creating and Deploying SSL Authentication for Nessus 100
Create Keys and User on Nessus Server 100
Create the nessuscert.pem Key 101
Configure Nessus Daemons 102
Change the Nessus Mode of Authentication 102
Using Custom Certificates 103
Deploy to other Nessus Scanners 103
Nessus Configuration for Windows 103
Commands and Relevant Files 103
Certificate Authority and Nessus Server Certificate 103
Nessus Client Keys 104
Creating and Deploying SSL Authentication for Nessus 104
Create Keys and User on Nessus Server 104
Transfer Certificates and Keys to SecurityCenter 106
Configure Nessus Daemons 107
Change the Nessus Mode of Authentication 107
Appendix 4: Using a Custom SSL Certificate 108
Appendix 5: Offline SecurityCenter Plugin Updates 109
Nessus 109
PVS (SecurityCenter 4.2 and greater only) 109
Appendix 6: Configuring LDAP with Multiple Organizational Units 110
Option 1 (Preferred) 110
Option 1 Example 110
Option 2 112
Option 2 Example 112
Appendix 7: Configuring SecurityCenter and the LCE for Audit Data Selection 114
About Tenable Network Security 117

Introduction

This document describes the administrative functions of Tenable Network Security's SecurityCenter 4.6.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 4.6 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there is some overlap in roles as well as content provided with each of the following guides:

- **SecurityCenter 4.6 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4. The target audience for this document is system administrators who need to install the SecurityCenter application. Included in this document are quick instructions for the **admin** user to add a Nessus scanner and create a user account to launch a test scan to ensure SecurityCenter is correctly installed.
- **SecurityCenter 4.6 Upgrade Guide** – This document describes the process of upgrading to the latest version of SecurityCenter 4.
- **SecurityCenter 4.6 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the **admin** user. The **admin** user is the first user to log in to the SecurityCenter after the initial installation and is responsible for configuration tasks such as defining organizations, repositories, Nessus scanners, LCE servers, and PVS sensors. The **admin** user does not have the ability to create and launch Nessus scans.
- **SecurityCenter 4.6 User Guide** – This document provides instructions for using SecurityCenter by an Organization Head user or lesser account.

Please email any comments and suggestions to support@tenable.com.

A basic understanding of Linux/Unix, Windows, vulnerability scanning with Nessus, intrusion detection, computer hardware, and log analysis is assumed.

Standards and Conventions

Throughout the documentation, filenames, daemons, and executables are indicated with a **courier bold** font such as **gunzip**, **httpd**, and **/etc/passwd**.

Command line options and keywords are also indicated with the **courier bold** font. Command line examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in courier (not bold). Following is an example running of the Unix **pwd** command:

```
# pwd
/opt/sc4/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples, and best practices are highlighted with this symbol and white on blue text.

Abbreviations

The following abbreviations are used throughout this documentation:

LCE	Log Correlation Engine
PVS	Passive Vulnerability Scanner
SC	SecurityCenter
SSH	Secure Shell
IDS	Intrusion Detection System

SecurityCenter Administrator Functions

SecurityCenter administrators have the following responsibilities:

- Manage the configuration of each SecurityCenter organization and which networks they are allowed to scan
- Manage scan policies, custom audit files, and credentials for all organizations
- Manage the network of active Nessus scanners, the network "zones" they belong to and the networks they are allowed to scan
- Manage the network of Passive Vulnerability Scanners and what organizations have access to their detected real-time vulnerabilities
- Manage which Log Correlation Engines each organization has access to and what repositories the LCE will correlate against
- Manage Log Correlation Engine Client configurations
- Delete accept and recast risk rules created by organizational users
- Manage what external data feeds (IDS information, PVS plugins, and Nessus plugins) SecurityCenter is subscribed to
- Manage the SecurityCenter services
- Add and manage other SecurityCenter administration users
- Add and manage custom roles that are available to all organizations
- Review SecurityCenter log files and job queues

Starting/Halting SecurityCenter

When SecurityCenter is installed and licensed, the required services are started by default. To display the status of SecurityCenter services, enter the following command as the root user on the SecurityCenter server:

```
# service SecurityCenter status
```

If SecurityCenter services are running, the following message will be displayed:

```
SecurityCenter (Jobd.php httpd) is running...
```

Otherwise, the message will state "`SecurityCenter is stopped`".

To start SecurityCenter, enter the following command:

```
# service SecurityCenter start
```

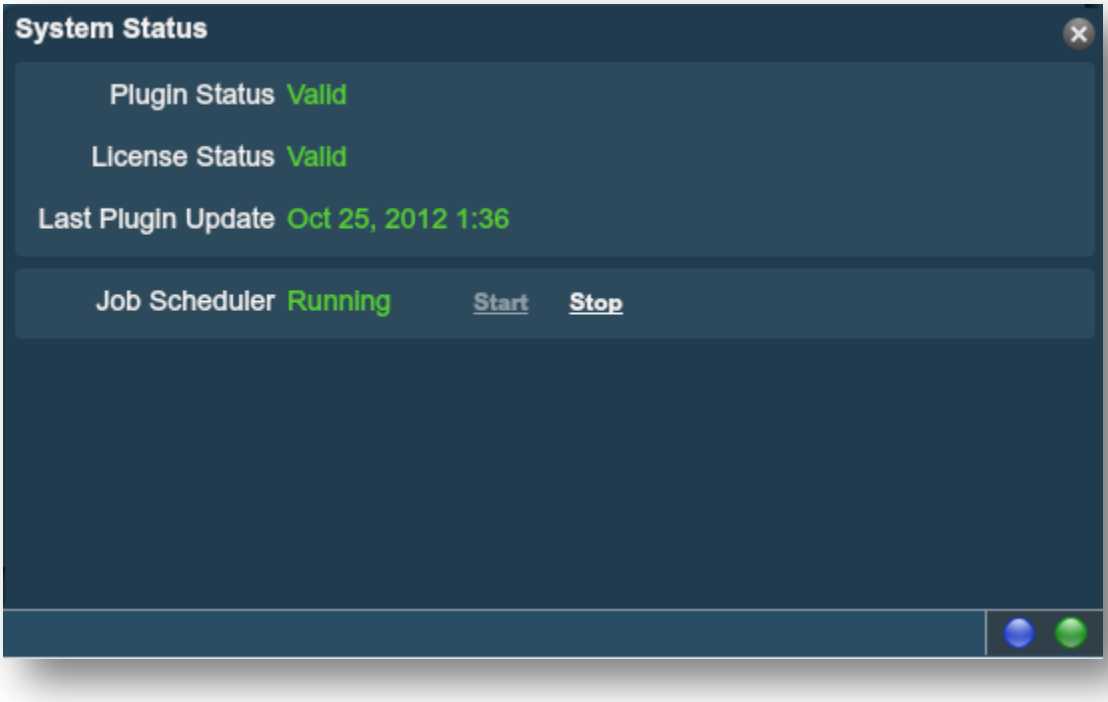
To halt SecurityCenter, enter the following command:

```
# service SecurityCenter stop
```

To restart SecurityCenter, enter the following command:

```
# service SecurityCenter restart
```

SecurityCenter services can also be started and stopped from the admin web management interface. Simply click the status circle (green in the image below) in the lower right-hand corner of the web page. A pop-up similar to the one below is displayed:



If the system status is normal, the circle is green and the "Job Scheduler" indicator shows "Running". Click "**Stop**" and then "**Start**" to restart the Job Scheduler process manually. If any known problems exist with SecurityCenter's status, they will be displayed on this pop-up and detailed in the logs described in the "Logs" section of this document.

SecurityCenter Home Page/Dashboard

To navigate within the SecurityCenter user interface, use the menu on the web interface screen, not the browser's back and forward arrow buttons.

Adobe Flash Player must be installed to use the SecurityCenter 4 web interface. It can be obtained at http://get.adobe.com/flashplayer/.

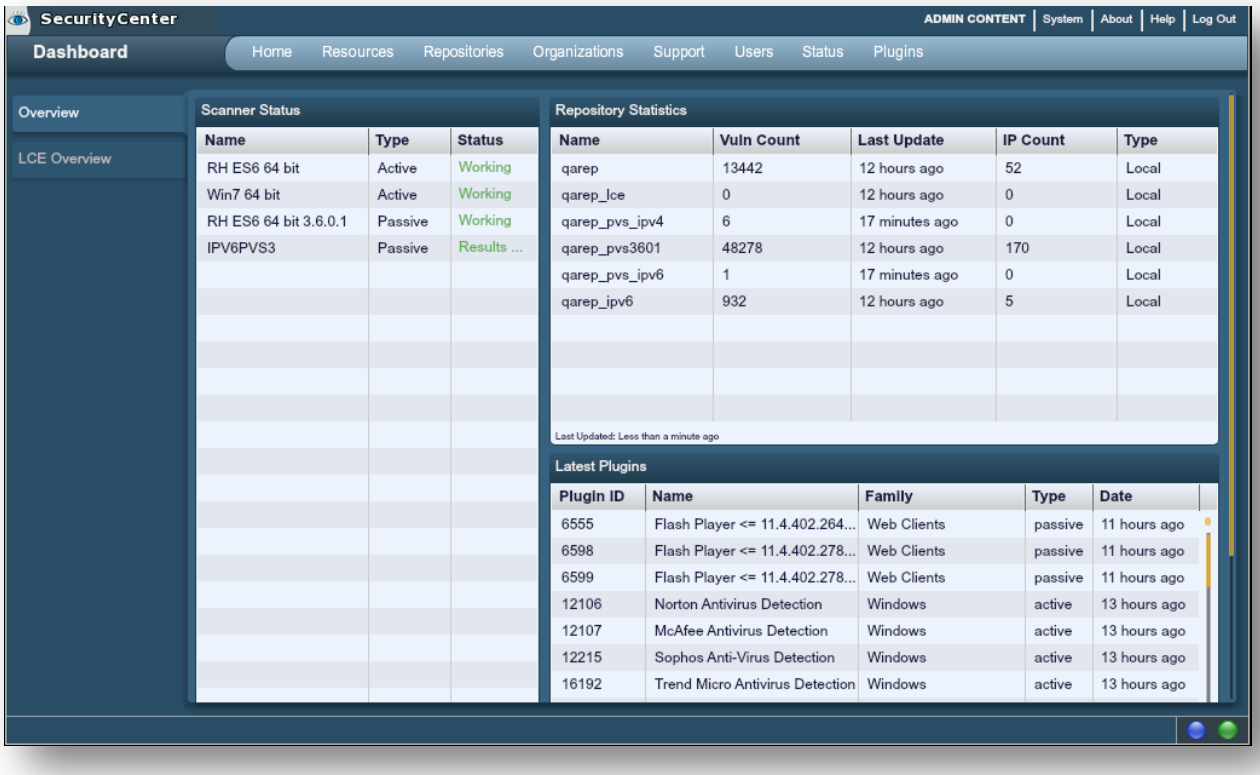
The minimum recommended browser window size is 1024x580. Resizing the browser window below this size when viewing the SecurityCenter web interface causes some items to display incorrectly.

To launch SecurityCenter, bring up a web browser on a system that has access to the SecurityCenter's network address space and enter the URL in the following format using SecurityCenter's IPv4 or IPv6 address or hostname:

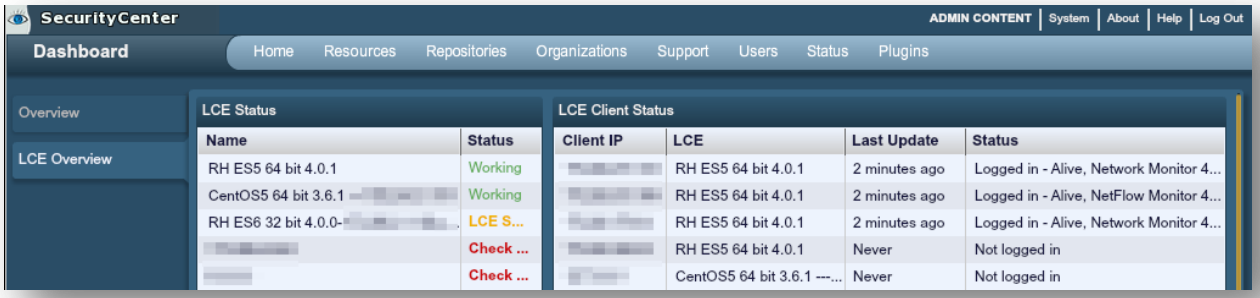
```
https://<SERVER ADDRESS OR NAME>/
```

The SecurityCenter web interface is available using a secure web connection (https). SecurityCenter 4 does not listen on port 80. TLS 1.0 must be enabled by the browser in order to complete the secure connection to SecurityCenter.

The dashboard is the first screen displayed when you log into the SecurityCenter user interface. It displays scanner, LCE, and plugin data through predefined components. The **Dashboard** can also be displayed by selecting "**Dashboard**" from the "**Home**" tab. There are two tabs: "**Overview**" and "**LCE Overview**". The **Overview** tab contains a Scanner Status table, a Repository Statistics table and a table containing the latest plugin feed updates. The **LCE Overview** tab lists the LCE servers and the status of clients attached to the LCE server (up to 1,000 clients displayed).


SecurityCenter
ADMIN CONTENT | System | About | Help | Log Out
Dashboard
Home Resources Repositories Organizations Support Users Status Plugins
Overview
LCE Overview
Scanner Status
Name Type Status
RH ES6 64 bit Active Working
Win7 64 bit Active Working
RH ES6 64 bit 3.6.0.1 Passive Working
IPV6PVS3 Passive Results ...
Repository Statistics
Name Vuln Count Last Update IP Count Type
qarep 13442 12 hours ago 52 Local
qarep_lce 0 12 hours ago 0 Local
qarep_pvs_ipv4 6 17 minutes ago 0 Local
qarep_pvs3601 48278 12 hours ago 170 Local
qarep_pvs_ipv6 1 17 minutes ago 0 Local
qarep_ipv6 932 12 hours ago 5 Local
Last Updated: Less than a minute ago
Latest Plugins
Plugin ID Name Family Type Date
6555 Flash Player <= 11.4.402.264... Web Clients passive 11 hours ago
6598 Flash Player <= 11.4.402.278... Web Clients passive 11 hours ago
6599 Flash Player <= 11.4.402.278... Web Clients passive 11 hours ago
12106 Norton Antivirus Detection Windows active 13 hours ago
12107 McAfee Antivirus Detection Windows active 13 hours ago
12215 Sophos Anti-Virus Detection Windows active 13 hours ago
16192 Trend Micro Antivirus Detection Windows active 13 hours ago

Sample SecurityCenter Administrator Dashboard – Overview



Sample SecurityCenter Administrator Dashboard – LCE Overview

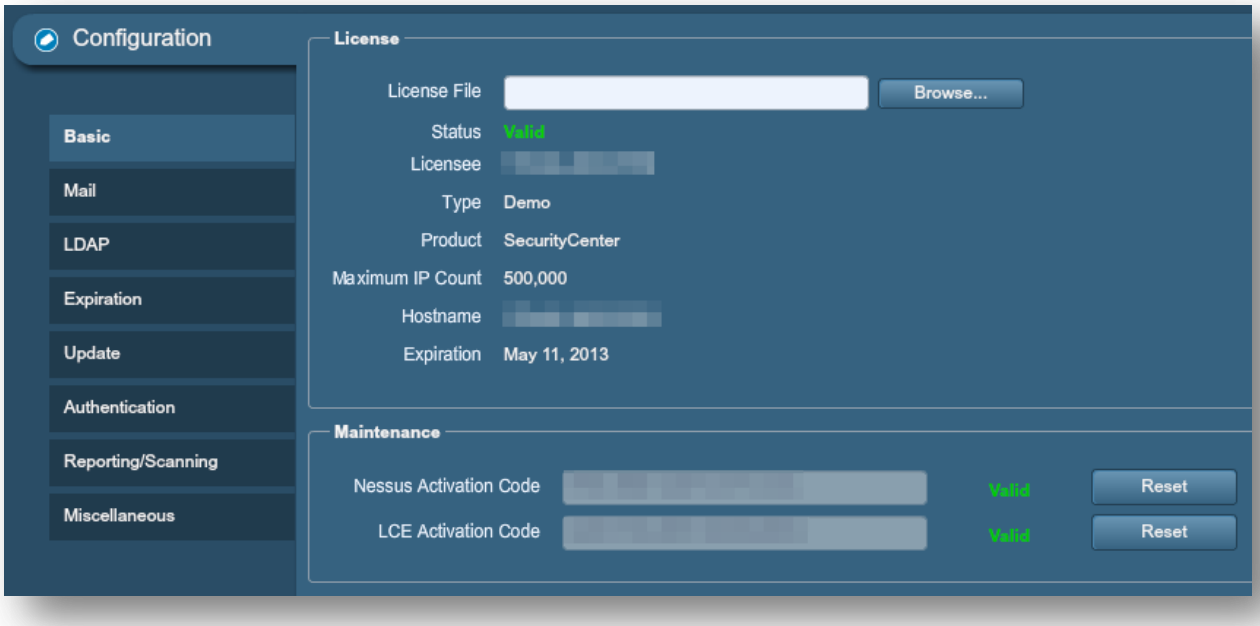
System Configuration

The "**System**" link at the top right of the SecurityCenter web interface contains a number of options to configure the desired SecurityCenter system behavior. When logged in as an admin user, additional options are available that are not available for non-admin users. Among the available admin options are "Basic" (licensing and activation), "Mail", "LDAP", "Expiration", "Update", "Authentication", and "Miscellaneous". The sections below provide details about each of the categories and their configuration items.

Configuration

Basic

The "Basic" options allow the admin user to configure the licensing and activation code settings for SecurityCenter. The screen capture below shows a sample SecurityCenter Basic option configuration page:



For most installations, this page will not be modified by the administrator, except when a new or upgraded IP Count license, Nessus Activation Code, or LCE Activation Code has been purchased by the organization and needs to be added.

To view currently used IPs in your license, log into SecurityCenter as the “admin” user and go to “Repositories” -> “Repositories”. Hover the cursor over the “Total Active IPs” graphic at the bottom of the screen to view currently used IPs, total IP license count, and IPs remaining.

Offline repositories are not counted against your IP license count. Also, the following plugins are not counted against your license IP count:
Nessus IDs: 10180, 10287, 19506, 12053, 11933
PVS IDs: 00003, 00012

To add a new license, use the “**Browse**” button next to the “**License**” field to locate the license key file received in your email and then click “**Submit**”.

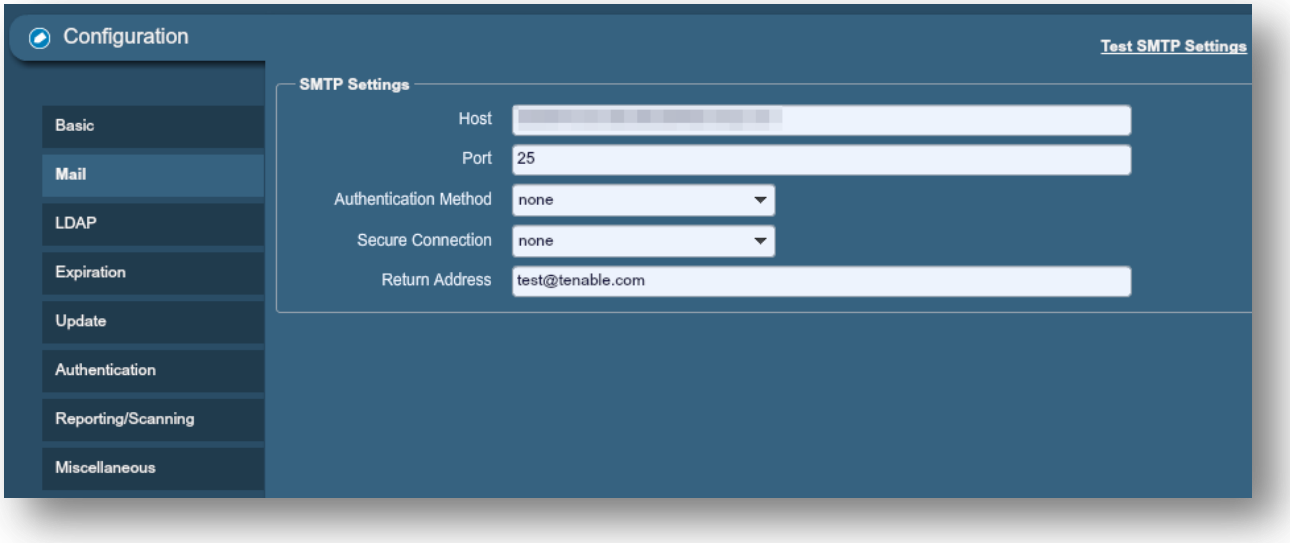
If replacing the Nessus Activation Code or LCE Activation code, in the Maintenance section first click “**Reset**” to allow the new Activation Code to be entered. Enter the new Activation Code in the appropriate field and click “**Register**”.

The current license status is displayed in the “License Status” field and indicates the current license state, licensee, type, product, maximum IP count allowed by the current license, the hostname that the license applies to and the expiration date, if any.

Mail

The “Mail” option designates SMTP settings for all email related functions of SecurityCenter. Available options include SMTP host, port, authentication method, secure connection and return address. In addition, a “Test SMTP Settings” link is displayed in the upper right-hand corner of the page to confirm the validity of the settings.

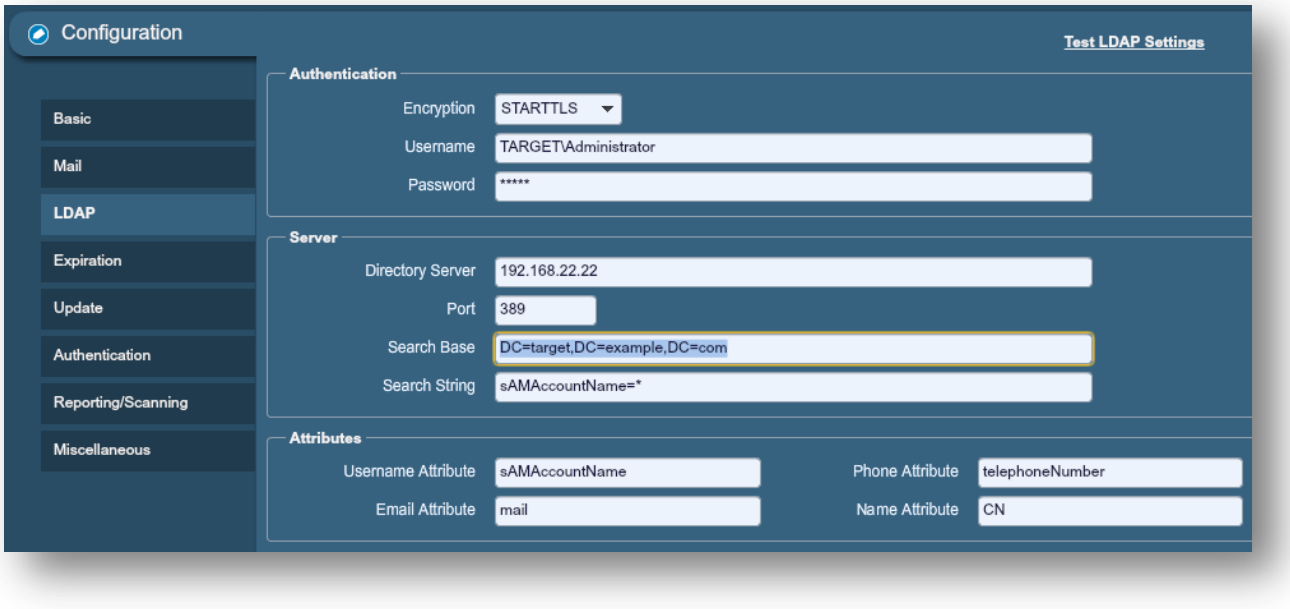
The “Return Address” defaults to “noreply@localhost”. Use a valid return email address for this field. If this field is cleared or the email server requires emails from valid accounts, the email will not be sent by the email server.



LDAP

If LDAP authentication is to be used, it is recommended to leave at least one SecurityCenter administrator account and one manager account for each organization in SecurityCenter set to use TNS authentication in the event that the LDAP services becomes unreachable.

LDAP configuration settings enable SecurityCenter to utilize any LDAP server for authentication purposes. This enhances the security of SecurityCenter by facilitating “single sign-on” and password complexity requirements in environments where mandated by security policy. After clicking the “LDAP” tab, a page similar to the one below is displayed.



Fill out the LDAP configuration settings as provided by the LDAP server administrator and click “Test LDAP Settings” to confirm the validity of the settings.

This table provides a detailed breakdown of the available LDAP parameters:

Table 1 – LDAP Directory Information

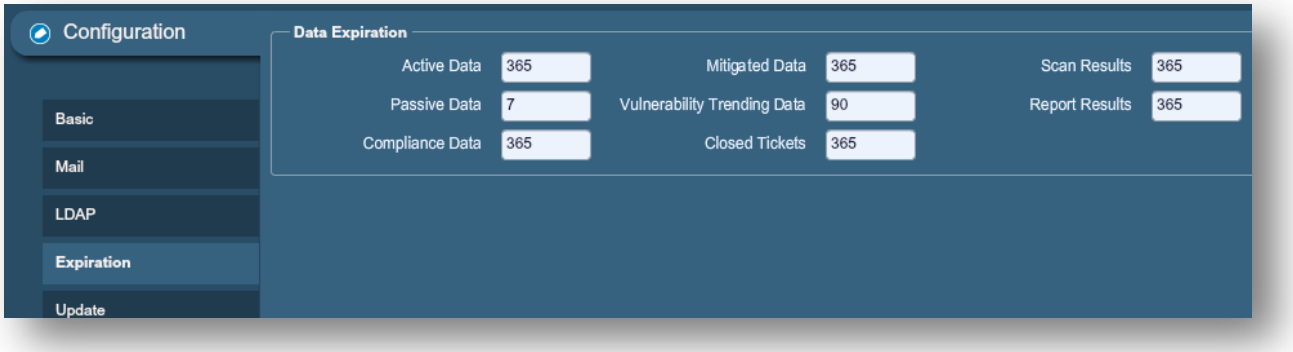
Option	Description
Authentication	
Authentication	This selection indicates if Transport Layer Security (TLS) or LDAP over SSL (LDAPS) is used for communication with the LDAP server.
Username	If the LDAP server requires credentials to search for user data, then the “Username” and “Password” fields are required. By default, if an Active Directory server is used for LDAP queries, it requires an authenticated search. Enter the username within this field in the “email” style format (user@domain.com).
Password (optional)	If the LDAP server requires credentials to search for user data, then the “Username” and “Password” fields are required. By default, many LDAP servers require an authenticated search.

	It is recommended to use passwords that meet stringent length and complexity requirements.
Server	
Directory Server	Enter the IP address or DNS name of the LDAP server in this field.
Port	Specify the remote LDAP port here. When Encryption is set to “none”, the LDAP port is typically 389, and when TLS or LDAPS is used, port 636 is the typical setting. Confirm the selection with your LDAP server administrators.
Search Base	This is the LDAP search base used as the starting point to search for the user information.
Search String	This string may be modified to create a search based on a location or filter other than the default search base or attribute.
Attributes	
Username Attribute	This is the attribute name on the LDAP server that contains the username for the account. This is often specified by the string “sAMAccountName” in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct username attribute to use.
Email Attribute	This is the attribute name on the LDAP server that contains the email address for the account. This is often specified by the string “mail” in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct email attribute to use.
Phone Attribute	This is the attribute name on the LDAP server that contains the telephone number for the account. This is often specified by the string “telephoneNumber” in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct telephone attribute to use.
Name Attribute	This field is the attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string “CN” in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct name attribute to use.

Access to Active Directory is performed via AD’s LDAP mode. When using multiple AD domains, LDAP access may be configured to go through the Global Catalog. Port 3268 is the default non-SSL/TLS setting, while port 3269 is used for SSL/TLS connections by default. More general information about LDAP searches via the Global Catalog may be found at: http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx

Expiration

Data expiration determines how long SecurityCenter retains acquired data.



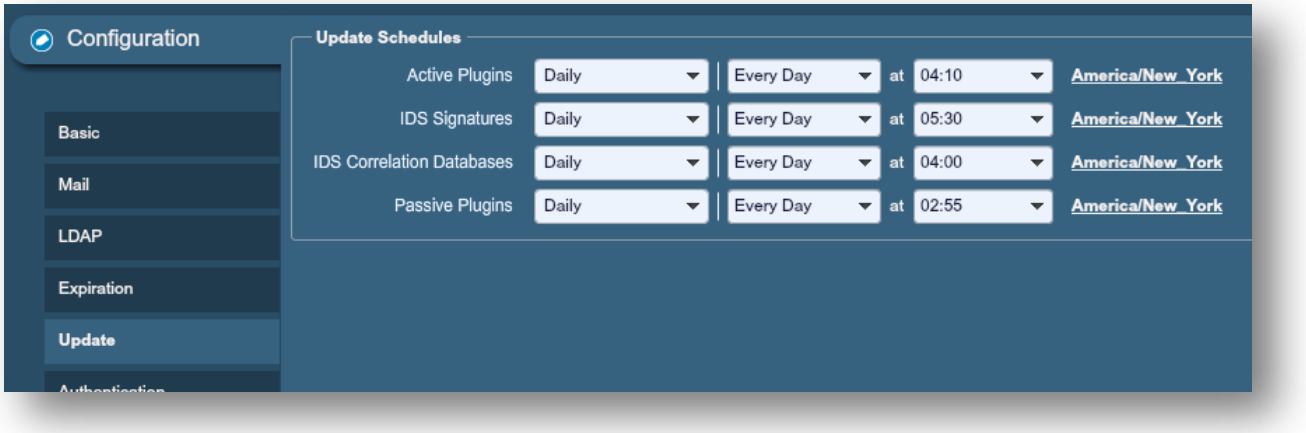
Use the table below to determine default and minimum values for these settings:

Table 2 – Data Expiration

Option	Description
Active Data	SecurityCenter will automatically remove any vulnerability data that was discovered via active scanning after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero (0). Setting this field to zero will remove all active vulnerabilities daily.
Passive Data	By default, SecurityCenter will automatically remove any passive vulnerability data that is older than seven days. If this field is left blank, the value will be set to zero (0). Setting this field to zero will remove all passive vulnerabilities daily.
Compliance Data	SecurityCenter will automatically remove any compliance data after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero (0). Setting this field to zero will remove all compliance vulnerabilities daily.
Mitigated Data	Automatically remove any mitigated vulnerability data after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero (0). Setting this field to zero will remove all mitigated vulnerability data daily.
Vulnerability Trending Data	Prior to SecurityCenter 4.2 the default was 365 days. Upgraded installations will maintain the 365 day default unless manually changed. SecurityCenter will automatically remove any vulnerability trending data after the designated number of days. The default value of this field is 90. This field must be greater than 0.
Closed Tickets	Automatically remove any closed tickets after the designated number of days. The default value of this field is 365. This field must be greater than 0.
Scan Results	Automatically remove any scan results after the designated number of days. The default value of this field is 365. This field must be greater than 0.
Report Results	Automatically remove any report results after the designated number of days. The default value of this field is 365. This field must be greater than 0.

Update

The SecurityCenter update settings are used to determine the update schedule for the common tasks of Active and Passive plugin updates, IDS signature updates, and IDS correlation updates. All updates are configured daily by default.



The following settings are available:

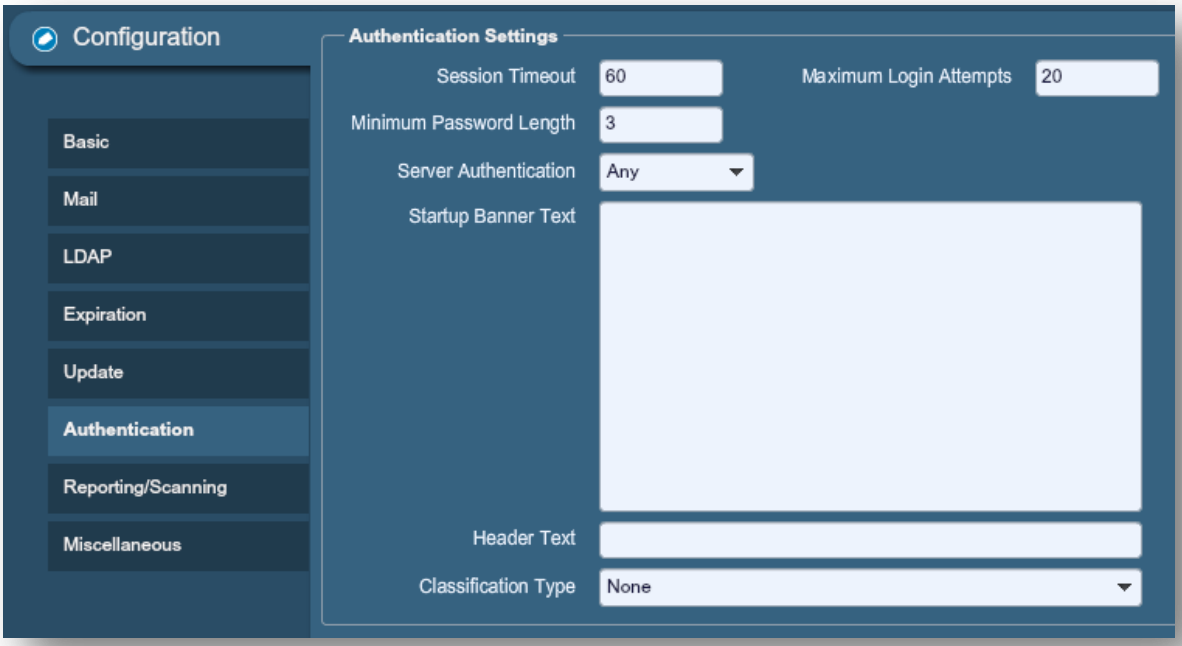
Table 3 – Update Schedules

Option	Description
Active Plugins	Enables regular downloads of the Nessus plugins. These plugins will be pushed out to every Nessus server that SecurityCenter is managing. Manual update of the Nessus plugins is also supported under the “Plugins” tab.
IDS Signatures	Frequency to update SecurityCenter IDS signatures via third-party sources.
IDS Correlation Databases	Frequency to push vulnerability information to the LCE for correlation.
Passive Plugins	Enables regular downloads of the PVS signatures. These plugins will be pushed out to every PVS that SecurityCenter is managing. Manual update of the PVS plugins is also supported under the “Plugins” tab.

Each of the update schedule times may also be configured to occur by time in a particular time zone, which can be selected via the “Time Zone” link next to each hour selection.

Authentication

“**Authentication Settings**” define the SecurityCenter web interface login parameters and options for account logins. Banners, headers, and classification headers and footers can also be configured from this screen.

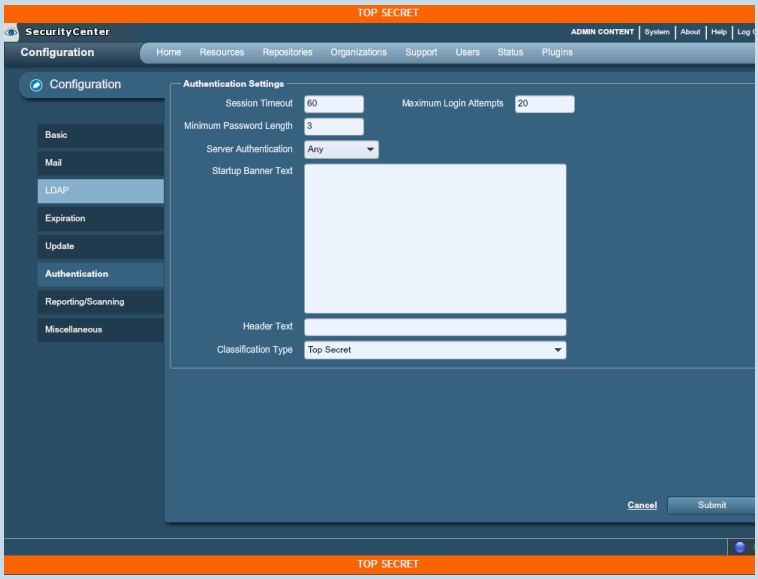


Use the table below to determine correct values for your environment:

Table 4 – SecurityCenter Authentication Settings

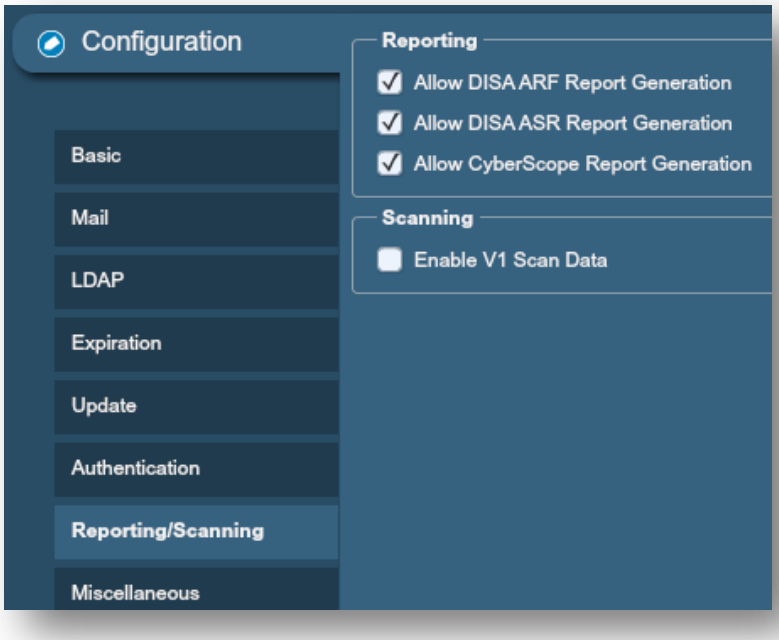
Option	Description
Session Timeout	The web session timeout in minutes (default: 60 minutes).
Maximum Login Attempts	The maximum number of user login attempts allowed by SecurityCenter before the account is locked out (default: 20). Setting this value to zero disables this feature.
Minimum Password Length	This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access (default:3).
Server Authentication	When set to "Any", any supported authentication method may be used except those listed in the drop-down menu. If a specific external Server Authentication method is selected from the drop-down list, only that method may be used to log into SecurityCenter. As of SecurityCenter 4.6, the only Server Authentication method available is CoSign. Please refer to the section titled "CoSign Configuration Instructions" for details on configuring CoSign.
Startup Banner Text	Enter the text banner that is displayed prior to the login interface.
Header Text	Adds custom text to the top of the SecurityCenter screen. The text may be used to identify the company, group, or other organizational information. The field is limited to 128 characters.

Classification Type	Adds a header and footer banner to SecurityCenter to indicate the classification of the data accessible via the software. Current options are “None”, “Unclassified”, “Confidential”, “Secret”, “Top Secret”, and “Top Secret – No Foreign”.



Reporting/Scanning

The Reporting/Scanning tab settings offers the option to enable or disable a variety of reporting types that are encountered and needed only in specific situations. The ability to enable or disable the use of Nessus V1 formatted files within SecurityCenter is set here as well.



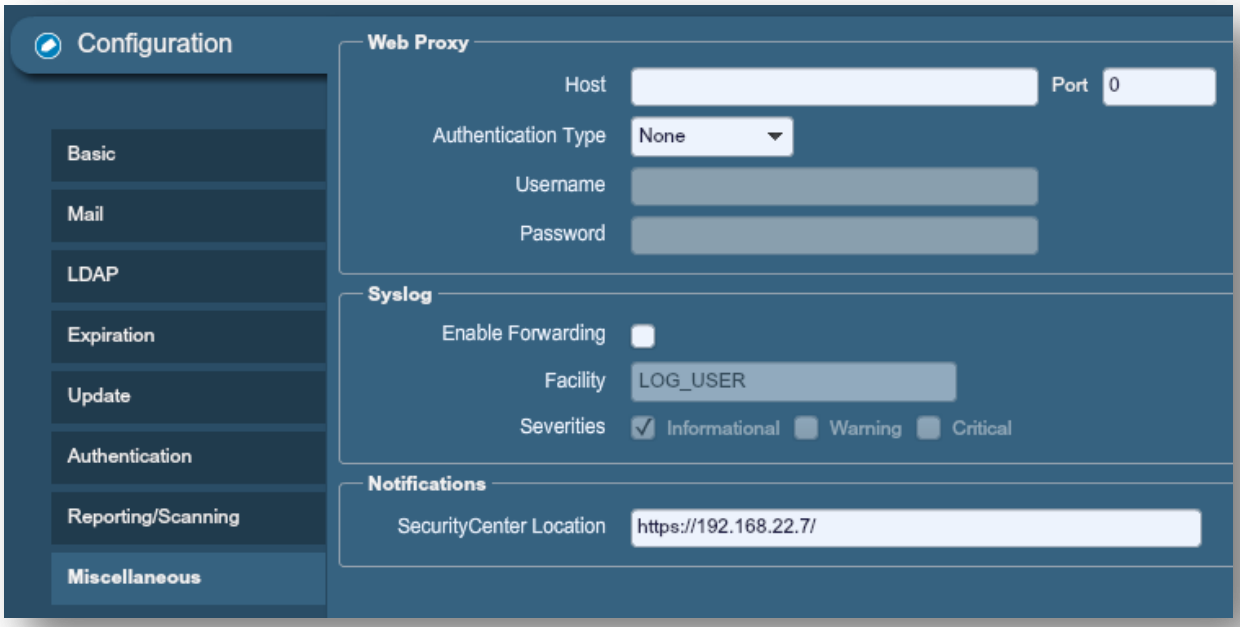
Among the reporting standards for the Defense Information Systems Agency (DISA) are the Asset Report Format (ASR) and the Assessment Results Format (ARF) styles. Additionally there is CyberScope reporting utilizing Lightweight Asset Summary Results Schema (LASR) style reports used by some segments of governments and industry. These formats are

typically used only by select groups and organizations for specific needs that do not apply to many organizations. The ability to enable or disable their usage within SecurityCenter is controlled here. Selecting the checkbox will enable the reporting type and unselecting will disable the reporting type in the report type drop-down for SecurityCenter users.

The “Scanning” section sets a global option to enable or disable the ability to download Nessus v1 data from Nessus scanners during scans. When enabled, Nessus scans will consume more disk space during an active scan. Downloading scan results from SecurityCenter in Nessus v1 format will only be available when this option is enabled.

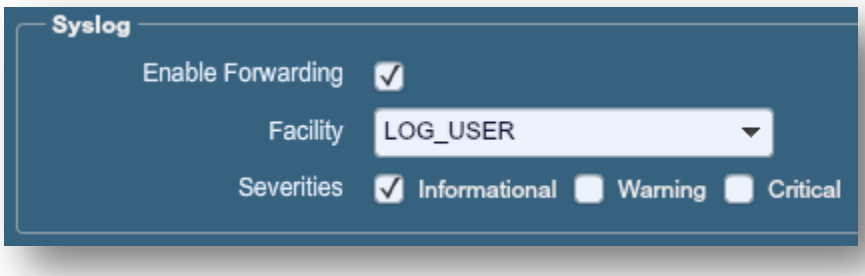
Miscellaneous

Miscellaneous settings cover web proxy setup, syslog, and Notifications. A sample SecurityCenter screen capture is included below:



From this configuration page, a web proxy can be configured by entering the host URL (protocol, proxy host name, or IP address), port, username, and password. The host name used must resolve properly from the SecurityCenter host.

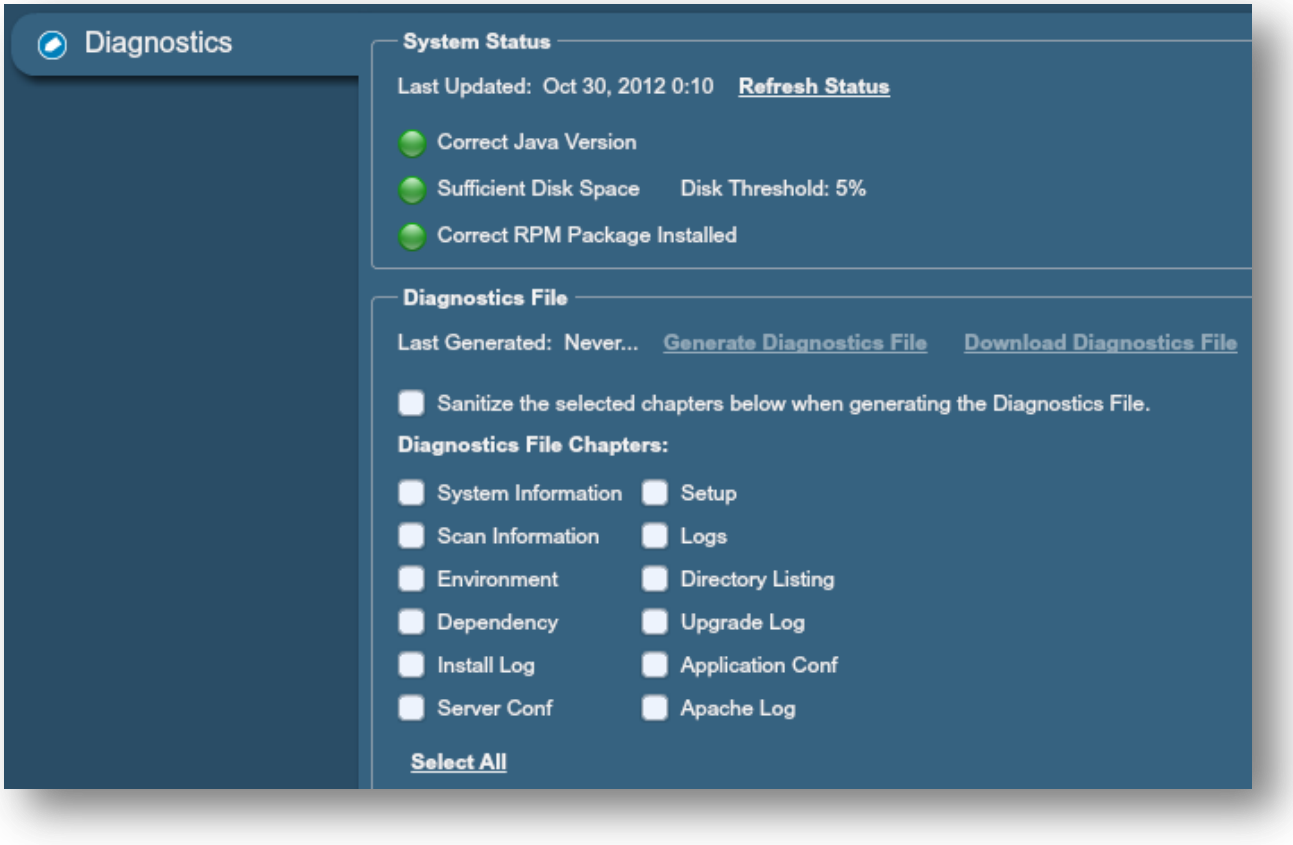
The “Syslog” section allows for the configuration and sending of SecurityCenter log events to the local syslog service. When “Enable Forwarding” is checked, the forwarding options are available for selection. The “Facility” drop-down provides the ability to select from the pre-defined facilities that will receive the log messages. The “Severities” section determines which level(s) of syslog messages will be sent: “Informational”, “Warning”, or “Critical”



The Notifications field defines the SecurityCenter web address used when notifications are generated for alerts and tickets.

Diagnostics

On the upper right-hand corner of the SecurityCenter web interface, the **System** option contains a drop-down that includes **Diagnostics**. This page displays and creates information that assists in troubleshooting issues that may arise while using SecurityCenter.



In the “System Status” section, the following items are indicated by a green icon for a properly working status. A red icon is displayed when the item is in a critical state.

Table 5 – System Status

Option	Description
Correct Java Version	The icon is red when a minimal version of Java is not installed as required by certain SecurityCenter features.
Sufficient Disk Space	Once the disk that stores the SecurityCenter data is within 5% of being filled, the icon indicator will turn red.
Correct RPM Package Installed	This indicator is green when the correct RPM is installed for the OS architecture on which it is running.

The “Diagnostics File” section is used primarily when working with the Tenable Support team. In order to troubleshoot issues that may be encountered, the Support team may request that a diagnostics file be generated with one or more of

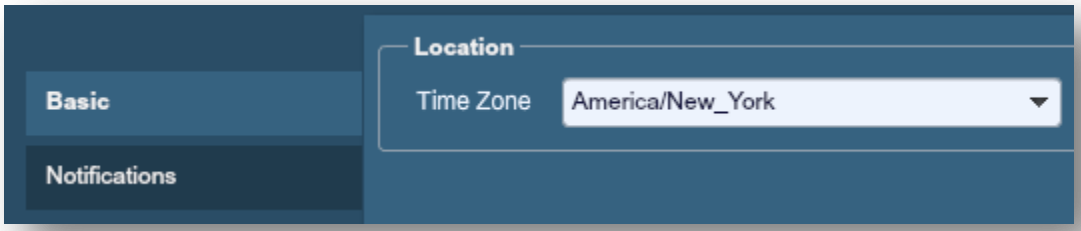
the “Diagnostics File Chapters” selected. If selected, the “Sanitize” option will remove IP addresses from the log files before generating the diagnostics file.

Preferences

On the upper right-hand of the SecurityCenter web interface, the **System** option contains a drop-down that includes **Preferences**. This option includes both location and notification settings.

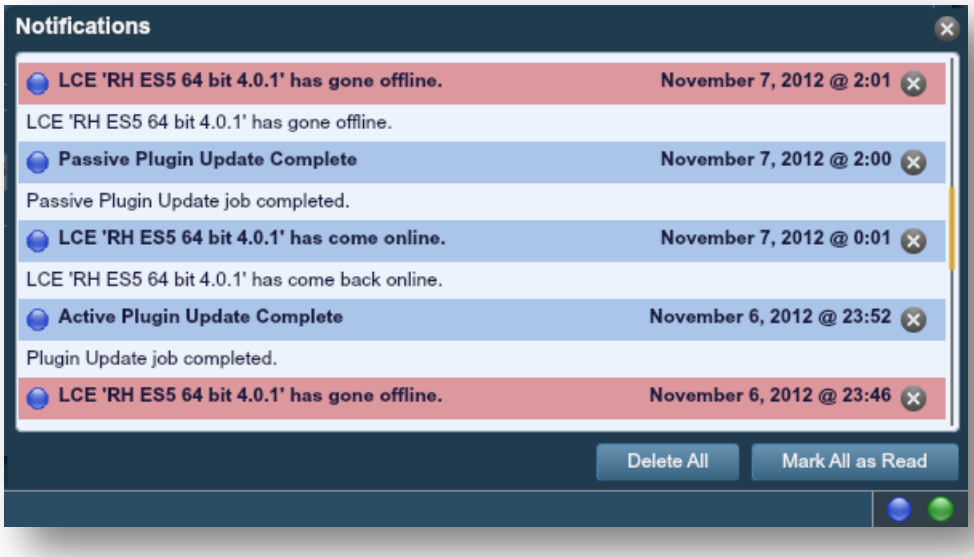
Basic

The “**Basic**” option tab allows the admin to configure the local time zone. **Important:** This affects the date/time displayed on reports and within the user interface and not the actual system time on the server itself.



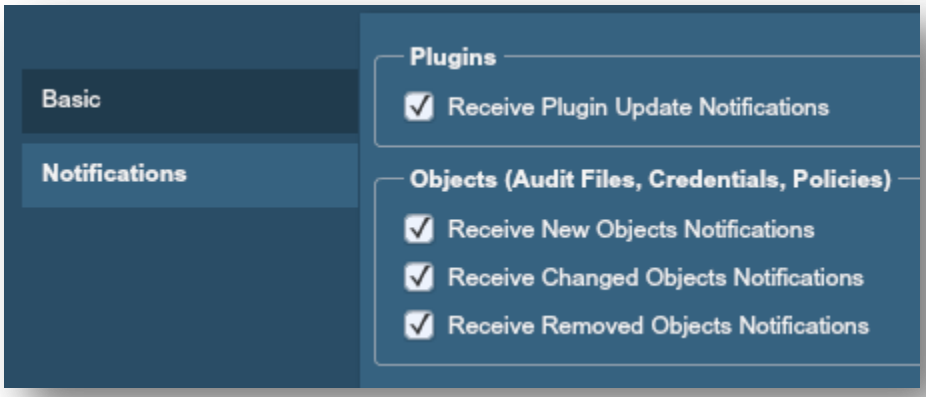
Notifications

Notifications are a feature of SecurityCenter that allows specified events to display a pop-up in the lower right-hand corner of the SecurityCenter web UI, as shown in the example below:


Notifications
LCE 'RH ES5 64 bit 4.0.1' has gone offline.
November 7, 2012 @ 2:01
LCE 'RH ES5 64 bit 4.0.1' has gone offline.
Passive Plugin Update Complete
November 7, 2012 @ 2:00
Passive Plugin Update job completed.
LCE 'RH ES5 64 bit 4.0.1' has come online.
November 7, 2012 @ 0:01
LCE 'RH ES5 64 bit 4.0.1' has come back online.
Active Plugin Update Complete
November 6, 2012 @ 23:52
Plugin Update job completed.
LCE 'RH ES5 64 bit 4.0.1' has gone offline.
November 6, 2012 @ 23:46
Delete All
Mark All as Read

Current notifications can be viewed by clicking on the left-hand circle at the lower right-hand corner of the SecurityCenter web page. Unread notifications will have a blue circle while a black circle indicates no unread notifications. Clicking on “**Mark All As Read**” removes the blue circle, but leaves the notifications there for later review. To view notification details, click the highlighted title to expand out the notification details.

Notifications can also be deleted by clicking on the “X” to the right of the notification text or clicking on the “**Delete All**” command button within the Notification box dialog. Admin configurable notifications are displayed in the screen capture below:

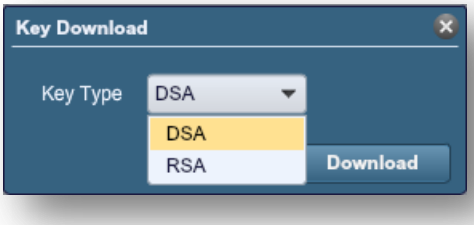


Keys

On the upper right-hand of the SecurityCenter web interface, the **System** option contains a drop-down that includes a **Keys** section. Keys allow the administrator to use key-based authentication with a remote SecurityCenter (remote repository) or between a SecurityCenter and an LCE server. This also removes the need for the SecurityCenter administrator to know the administrator login or password of the remote system.

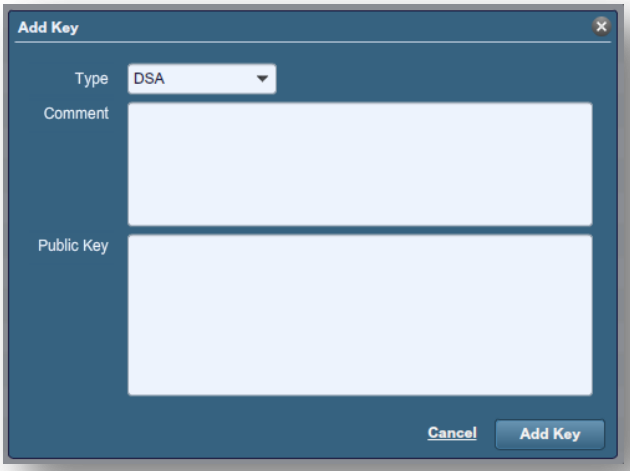
The public key from the local SecurityCenter must be added to the "Keys" section of the SecurityCenter that you wish to retrieve a repository from. If the keys are not added properly, the remote repository "add" process will prompt for the root username and password of the remote host before the repository add/sync occurs.

Available options include "**Download Key**", "**Add**", and "**Delete**". To download the local SecurityCenter's key, click "**Download Key**". After doing this, the key format dialog is displayed. Choose the type of key being requested and then click "**Download**":



If "DSA Key" was chosen during download, the DSA public key is downloaded. Likewise, choosing "RSA Key" downloads the RSA public key string.

Clicking on "**Add**" brings up the dialog box below:



In the "Type" drop-down, select DSA or RSA as the key type.

In the "Comment" box, enter a string of text that describes the purpose of the key being added to the system.

In the "Public Key" box, paste the text of the public key from the remote SecurityCenter and click "Submit". If a valid public key was entered, a "Success" message is displayed and the key will show up in the key list.

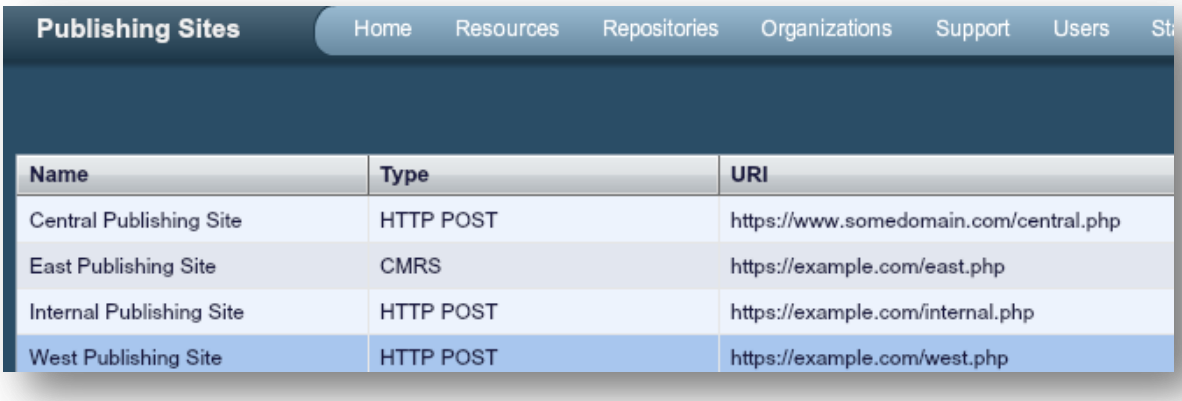
Remote LCE Key Exchange

A manual key exchange between the SecurityCenter and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote LCE to recognize the SecurityCenter, you need to copy the SSH public key of the SecurityCenter and append it to the "`/opt/lce/.ssh/authorized_keys`" file. The "`/opt/lce/daemons/lce-install-key.sh`" script performs this function. The steps are outlined in Appendix 2 of this document.

Publishing Sites

Organizations may configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site.



Configuring the publishing sites starts with clicking the “Add” button to open the “Add Publishing Site” window as shown below:

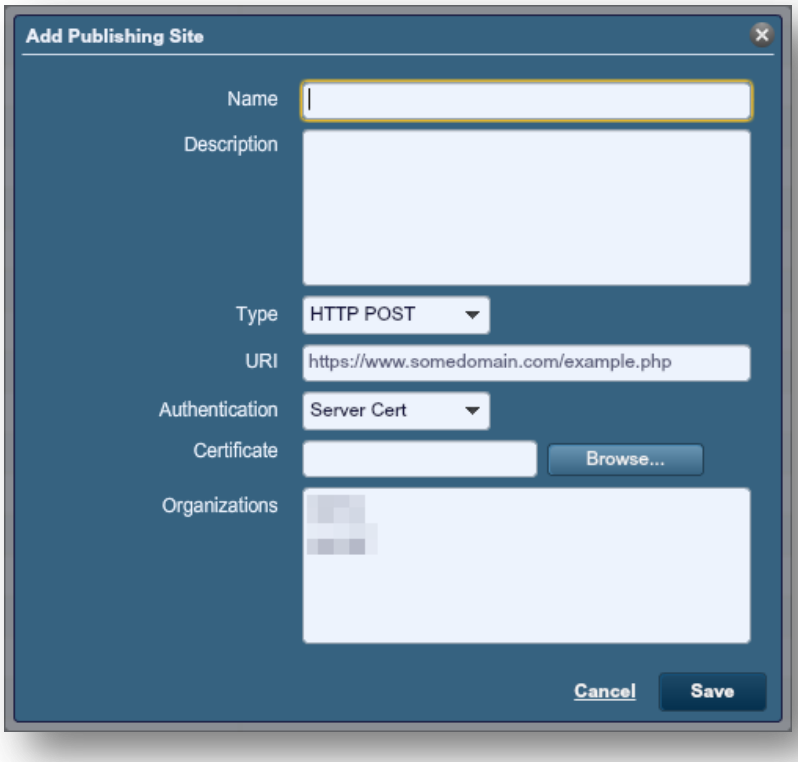


Table 6 – Publishing Site Options

Option	Description
Name	Enter a name for the publishing site.
Description	Enter a description of the publishing site.
Type	This is the method SecurityCenter will use to publish to the site. Available options are “HTTP Post” or “CMRS”. Use the selection appropriate for the configuration of the publishing site.
Max Chunk Size (MB) (CMRS Only)	When set to a non-zero number, files will be sent to the publishing site in parts, or ‘chunked’, in the configured file size.
URI	This is the target address to send the report to when completed.
Authentication	There are two methods of authentication available. One is “Server Cert” and the other is “Password”. When “Server Cert” is selected, the option to upload a certificate is available. When “Password” is selected, fields are available to enter a username and password to authenticate to the publishing server.
Organizations	This field allows for selecting the Organization(s) that are allowed to publish to the configured site.

SSL Client Certificate Authentication

SecurityCenter 4.6 allows users to use SSL client certificate authentication. This allows use of SSL client certificates, smart cards, and CAC authentication when the browser is configured for this method.

By default, SecurityCenter uses a password to authenticate. To configure SecurityCenter to allow SSL client certificate authentication the web server must be configured to allow such connections. To do this, the **`/opt/sc4/support/conf/sslverify.conf`** file must be edited on the SecurityCenter server using any standard text editor. Edit the "**`SSLVerifyClient`**" setting to use an option of **`none`**, **`optional`**, and **`require`** as described in the following table.

Table 7 – SSL Client Certificate Configuration Options

Option	Description
none	When set to "none", SSL certificates for SecurityCenter will not be accepted by the server for user authentication purposes.
optional	When set to "optional", valid SSL certificates for SecurityCenter may be used for user authentication. If a valid certificate is not presented, the user may log in using only a password. Depending on how they are configured, some web browsers may not connect to SecurityCenter when the "optional" setting is used.
require	When set to "require", a valid SSL certificate for SecurityCenter must be presented to gain access to the web interface. If the user has an account that uses a certificate to authenticate, that user will be logged into SecurityCenter. Otherwise the user will be presented with the standard SecurityCenter login page.

When a user is initially created and configured, a password must be created for the user. Users who are configured to use SSL certificates will be prompted to determine if they want to always use the current certificate when they log in to SecurityCenter through a browser. If "Yes" is selected, the certificate will be associated with their account and future access to SecurityCenter will use the client certificate. If "No" is selected, the certificate will be ignored for the current session.

Configure SecurityCenter for Certificates

The first step to allow SSL certificate authentication is to configure the SecurityCenter web server. This process allows the web server to trust certificates created by the Certificate Authority (CA) for authentication.

1. Copy the required PEM-encoded CA certificate (and intermediary CA, if needed) to the SecurityCenter server's **`/tmp`** directory. For this example, the file is named **`ROOTCA2.cer`**.

2. Run the **`installCA.php`** script to create the required files for each CA in **`/opt/sc4/data/CA`** as follows:

   ```
   # /opt/sc4/support/bin/php /opt/sc4/src/tools/installCA.php /tmp/ROOTCA2.cer
   ```

3. Once each of your CAs has been processed, restart the SecurityCenter services with the following command:

   ```
   # service SecurityCenter restart
   ```

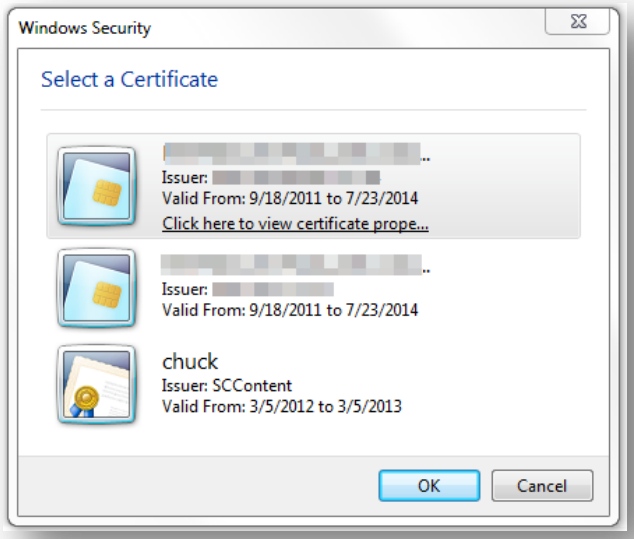
After SecurityCenter has been configured with the proper CA certificate(s), users may log in to SecurityCenter using SSL client certificates.

Connect with SSL Certificate Enabled Browser

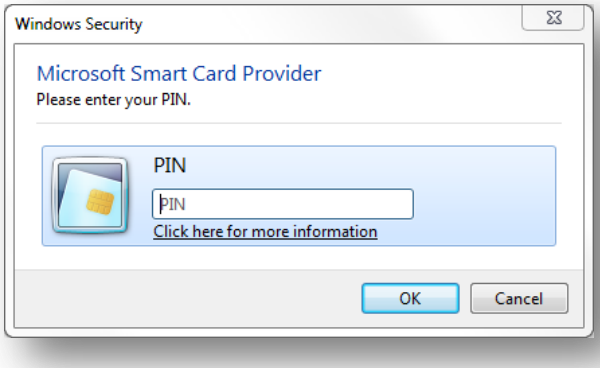
The following information is provided with the understanding that your browser is configured for SSL certificate authentication. Please refer to your browser's help files or other documentation to configure this feature.

The process to configure a certificate login begins when a user connects to SecurityCenter for the first time. The process is completed by the user and does not require Administrator intervention.

1. Launch a browser and navigate to SecurityCenter.
2. The browser will present a list of available certificate identities to select from:



3. Once a certificate has been selected, a prompt for the PIN or password for the certificate is presented (if required) to access your certificate. When the PIN or password is successfully entered, the certificate will be available for the current session with SecurityCenter.

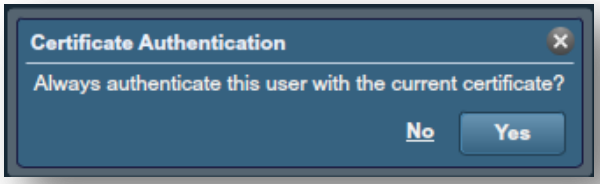


4. Upon the initial connection, log in using the username to be associated with the selected certificate.

Only one SecurityCenter user may be associated with a single certificate. If one user holds multiple user names and roles, a unique certificate must be provided for each login name.

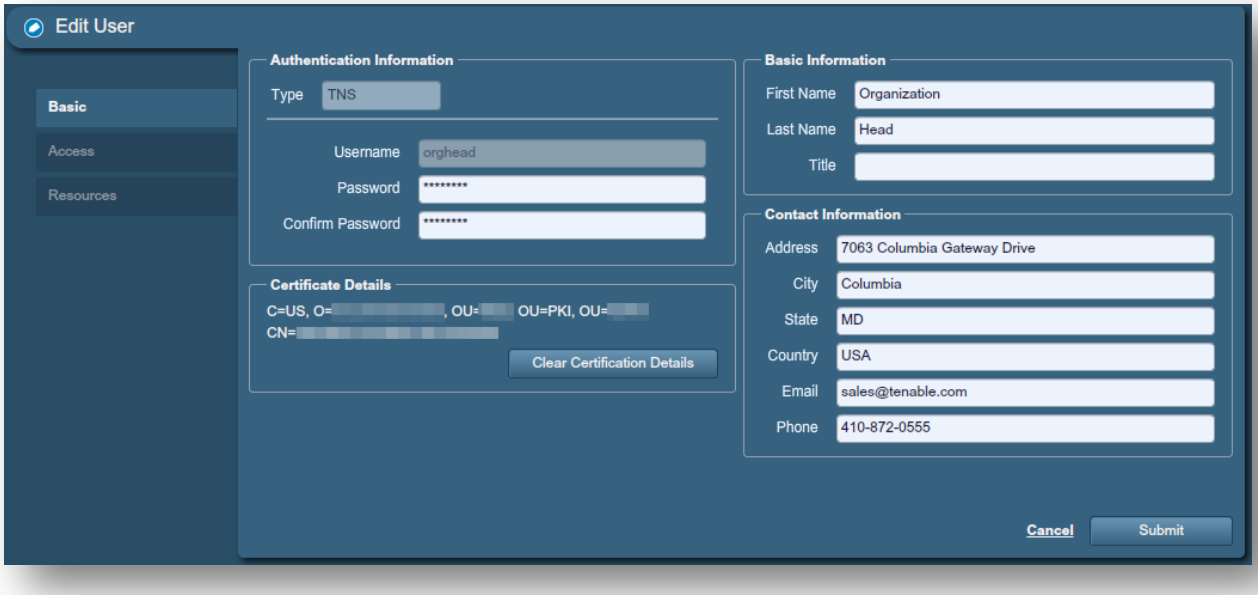
5. Once logged in, a window titled “Certificate Authentication” is presented, asking if the current certificate is to be used to authenticate the current user. If “Yes” is selected, the certificate will be associated with this user. If “No” is selected, the certificate will be ignored for the current session.

If the user’s browser is configured for certificate authentication but is not configured for a SecurityCenter user, the following prompt will be presented for each login.

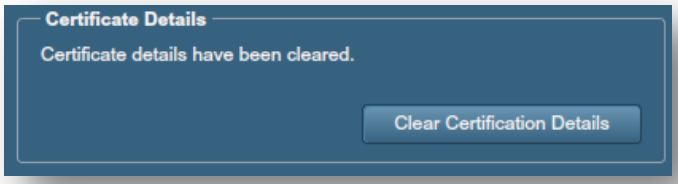


6. When a user’s account is associated with a certificate, it is displayed on the user’s information page and may be viewed using the “Edit User” page on the “Basic” tab.

The “Certificate Details” section for a user only appears if there is an associated certificate.



7. If a user’s certificate changes or is required to be revoked, the current certificate may be disassociated from the user by clicking the “Clear Certification Details” button. The current information will be deleted and replaced with the following until a new certificate is submitted:



8. If a new certificate is available the next time the user logs in, SecurityCenter will again attempt to associate the user with the certificate.

If you log out of the session, you will be presented with the standard SecurityCenter login screen. If you wish to log in again with the same certificate, refresh your browser window. If you need to use a different certificate, you must restart your browser session.

CoSign Configuration Instructions

Misconfiguration of the CoSign authentication configuration can cause you to lose access to SecurityCenter. Please contact Tenable Support for possible recovery options.

The information presented in this section assumes an existing, working CoSign service solution. More information about CoSign authentication servers may be found at http://weblogin.org.

SecurityCenter 4.6 introduces a new server authentication method that uses the CoSign single sign-on solution. Once enabled, the TNS and LDAP authentication methods are no longer available for use. SecurityCenter 4.6.0 only supports username/password authentication via CoSign; support for additional methods may be added later.

If CoSign authentication is enabled, usernames in SecurityCenter must be matched to those in the CoSign system. Before enabling CoSign authentication, ensure that at least one administrator-level user exists with an acceptable username for CoSign authentication. If a user exists within SecurityCenter without a matching CoSign user, access to that user will be lost after the conversion to CoSign authentication.

The first step to configuring CoSign authentication is to install a valid SSL CA certificate and a client SSL certificate and key provided by your CoSign administrator in a .pem format. Copy this key to the SecurityCenter server, as the user 'tns' ("`su - tns`") and run the command:

```
# /opt/sc4/support/bin/php /opt/sc4/src/tools/installCA.php /path/to/consign_ca.pem
```

This allows SecurityCenter to install the CA certificate with the appropriate permissions to enable secure communication between the SecurityCenter server and the CoSign server. Copy the client SSL certificate and key files to the **`/opt/sc4/support/cosign`** directory. Ensure that the ownership of the files is tns:tns and its permissions allow the owner to at least read the file. For example, if the files are named modcosign.crt and mod_cosign.key, the following commands will set the ownership correctly:

```
# chown tns:tns /opt/sc4/support/cosign mod_cosign.crt
# chown tns:tns /opt/sc4/support/cosign mod_cosign.key
```

Next, the Apache CoSign module must be enabled. Edit the **`/opt/sc4/support/conf/module.conf`** file using any standard text editor to enable the mod_cosign.so module by removing the # at the beginning of the line as follows:

```
LoadModule cosign_module modules/mod_cosign.so
```

Next, SecurityCenter's **/opt/sc4/support/conf/cosign.conf** must be edited for the correct settings for your environment. In the following example, 192.168.5.5 is used as the CoSign server's IP address and 192.168.7.44 is the IP address of the SecurityCenter server. Only the configured lines of the configuration file are displayed.

The configuration below is an example only. Please obtain the correct configuration parameters for your environment from your CoSign administrator.

```
CosignProtected off
CosignHostname 192.168.5.5
CosignCrypto /opt/sc4/support/cosign/mod_cosign.key
       /opt/sc4/support/cosign/mod_cosign.crt /opt/sc4/data/CA
CosignFilterDB /opt/sc4/support/cosign/filter
CosignCheckIP never
CosignService tenable
CosignRedirect https://192.168.5.5
CosignPostErrorRedirect https://192.168.5.5/post_error.html
CosignValidReference ^https?:\/\/192.168.7.44(\/.*)?
CosignValidationErrorRedirect https://192.168.5.5/invalid.html
CosignRequireFactor factor.sh
<Location /cosign/valid>
SetHandler cosign
CosignProtected Off
CosignValidReference ^https?:\/\/192.168.5.5(\/.*)?
CosignValidationErrorRedirect https://192.168.5.5/invalid.html
Allow from all
Satisfy Any
</Location>
```

Once the configuration file has been configured appropriately, the next step is to configure SecurityCenter to use CoSign authentication. Log in as an admin user, navigate to the "Configuration" page and go to the "Authentication" tab. Under the Server Authentication drop-down, select "CoSign" and submit.

After making the above changes, restart the SecurityCenter service with the "**service SecurityCenter restart**" command to enable CoSign authentication for SecurityCenter. When navigating to the SecurityCenter server, you will initially be redirected to the CoSign server for authentication. Once authenticated on the CoSign server, the log into SecurityCenter will be completed.

Resource Management

The **Resources** tab provides the Admin user with the ability to configure supporting resources such as Log Correlation Engines, Nessus scanners (and scan zones), and Passive Vulnerability Scanners. This section describes the various resources and configuration options.

Nessus Scanners

In the SecurityCenter framework, the Nessus scanner behaves as a server, while SecurityCenter serves as a client that schedules and initiates scans, retrieves results, reports results, and performs a wide variety of other important functions. Click "**Resources**" and then "**Nessus Scanners**" to retrieve a list of the scanners and their current status, version, host, number of assigned zones, and when they were last modified. If the status of a scanner has changed recently (since visiting the page), click the "**Update Status**" button to see the latest scanner status.

There are three classifications of Nessus scanners that may be added to SecurityCenter: "**Managed**", "**Unmanaged**", and "**Perimeter Service**".

Managed
A "**Managed**" scanner is one that is managed by SecurityCenter. Managed scanners are logged into using Nessus admin credentials, and SecurityCenter has the ability to send plugin updates to the scanner. SecurityCenter also maintains the Activation Code for Managed scanners.

Unmanaged
An "**Unmanaged**" scanner is one that has been logged into using a standard Nessus user's credentials. This scanner may be used to perform a scan but SecurityCenter cannot send plugin updates to an unmanaged scanner or manage its Activation Code.

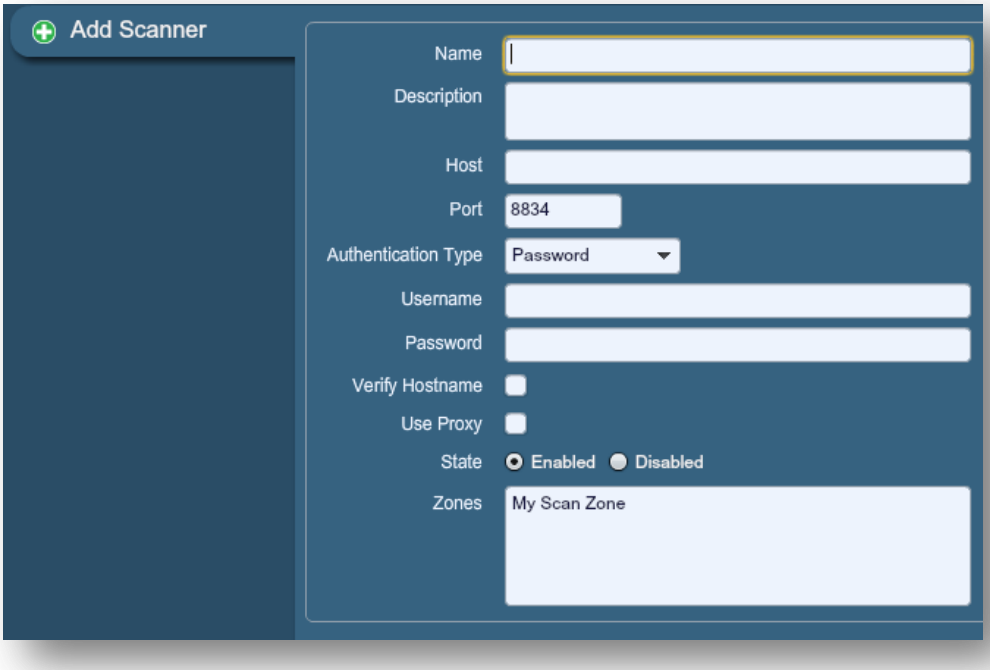
Perimeter Service
SecurityCenter may also use a "**Perimeter Service**" scanner to perform scans using Tenable's Perimeter Service. This is a vulnerability scanning service that may be used to audit Internet facing IP addresses for both network and web application vulnerabilities "from the cloud". The Perimeter Service is also considered to be an unmanaged scanner, and SecurityCenter will not push plugin updates to a Perimeter Service scanner. More information about using the Perimeter Service through SecurityCenter is found in the Nessus Perimeter Service Scanners section of this document.

In the examples below, the Nessus scanners are installed on remote systems, are of varying types, and are functioning properly.

Name	Host	# of Zones	Status	Version	Type	Last Modified
DMZ Scanner	nessushost2	1	Working	5.0.2 (Web: 4.0.7)	Unmanaged	1 minute ago
Internal Scanner	nessushost	1	Working	5.0.2 (Web: 4.0.7)	Managed	6 days ago
Perimeter Service Scanner	[redacted]	1	Working	5.0.2 (Web: 4.0.6)	Perimeter Service	3 hours ago

Adding a Nessus Scanner

To add a scanner, click the "**Add**" button. A screen capture of the "Add Scanner" dialog is shown below:



The table below goes into more detail about the available options for adding a Nessus scanner:

Table 8 – Nessus Scanner Options

Option	Description
Name	Descriptive name for the Nessus scanner.
Description	Scanner description, location, or purpose.
Host	Hostname or IP address of the scanner.
Port	TCP port that the Nessus scanner listens on for communications from SecurityCenter. The default is port 8834.
Authentication Type	Password Based or SSL Certificate. For detailed SSL Certificate configuration options, see Appendix 3: Nessus SSL Configuration.
Username	Username generated during the Nessus install for daemon to client communications. This must be an administrator user in order to send plugin updates to the Nessus scanner. If the scanner will be updated by a different method, such as through another SecurityCenter, a standard Nessus user account may be used to perform scans. This field is only available if the Authentication Type is set to "Password".
Password	The login password must be entered in this field. This field is only available if the Authentication Type is set to "Password".
Certificate	This field is available if the Authentication Type is "SSL Certificate". Select the "Browse" button, choose a SSL Certificate file to upload, and upload to the SecurityCenter. For more information, see Appendix 3: Nessus SSL Configuration.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the "Host" field matches the CommonName (CN) presented in the SSL certificate from the Nessus server.
Use Proxy	Instructs SecurityCenter to use its configured proxy for communication with the scanner.
State	A scanner may be marked as "Enabled" or "Disabled" within SecurityCenter to allow or prevent access to the scanner.
Zones	The zone(s) that will have access to use this scanner.

Configure SecurityCenter for Custom Certificates to Verify Hostname

The first step to allow the Verify Hostname to work is to ensure the correct Certificate Authority (CA) certificate is configured for use by SecurityCenter. When using the default certificates for Nessus servers, this is not required to be done. Only when a custom CA is in use do these steps need to be performed.

1. Copy the required PEM-encoded CA certificate (and intermediary CA, if needed) to the SecurityCenter server's **`/tmp`** directory. For this example, the file is named **`ROOTCA2.cer`**.

2. Run the **`installCA.php`** script to create the required files for each CA in **`/opt/sc4/data/CA`** as follows:

   ```
   # /opt/sc4/support/bin/php /opt/sc4/src/tools/installCA.php /tmp/ROOTCA2.cer
   ```

3. Once each of your CAs has been processed, restart the SecurityCenter services with the following command:

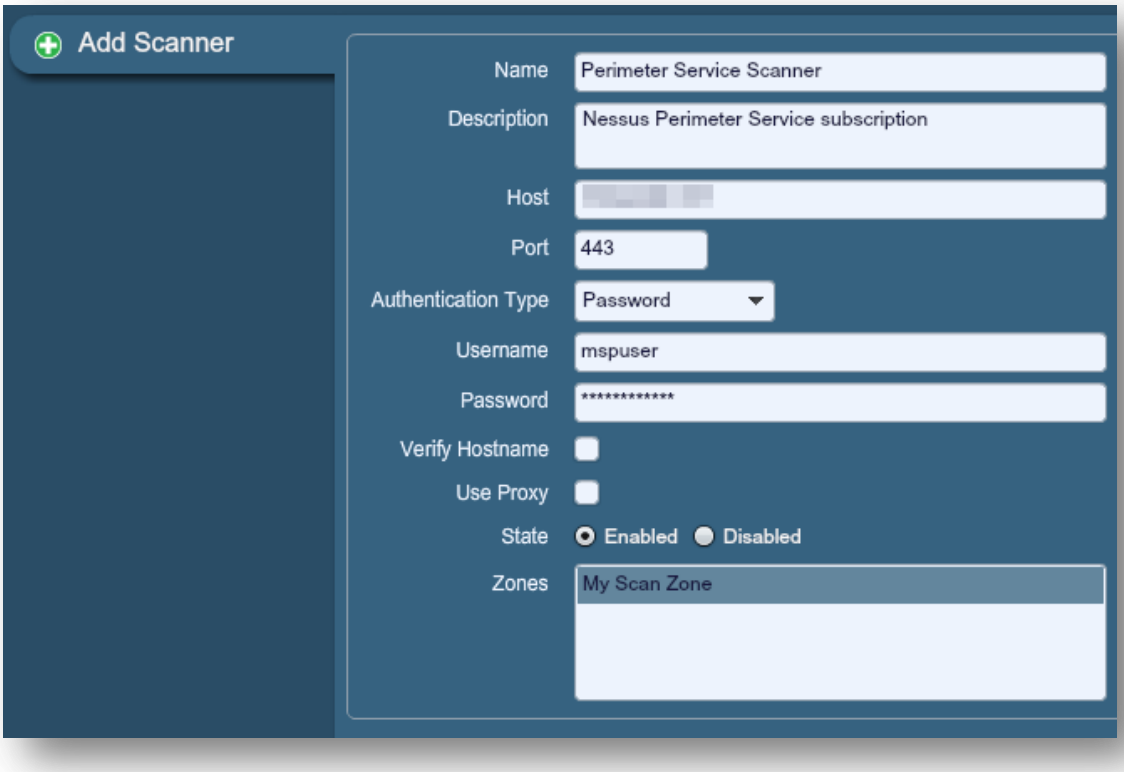
```
# service SecurityCenter restart
```

After SecurityCenter has been configured with the proper CA certificate(s), the Verify Hostname will verify the SSL certificate presented against the proper CA certificate.

Nessus Perimeter Service Scanners

SecurityCenter 4.6 supports the use of the **Nessus Perimeter Service** as a Nessus scanner within SecurityCenter. The Nessus Perimeter Service is an enterprise-class remote vulnerability scanning service that may be used to audit Internet facing IP addresses for both network and web application vulnerabilities “from the cloud”. While they are not “managed” by a SecurityCenter (e.g., plugins are not pushed from SecurityCenter to the scanner), Nessus Perimeter Service scanners can be added to SecurityCenter in the same manner that internal, local, or remote Nessus scanners are added.

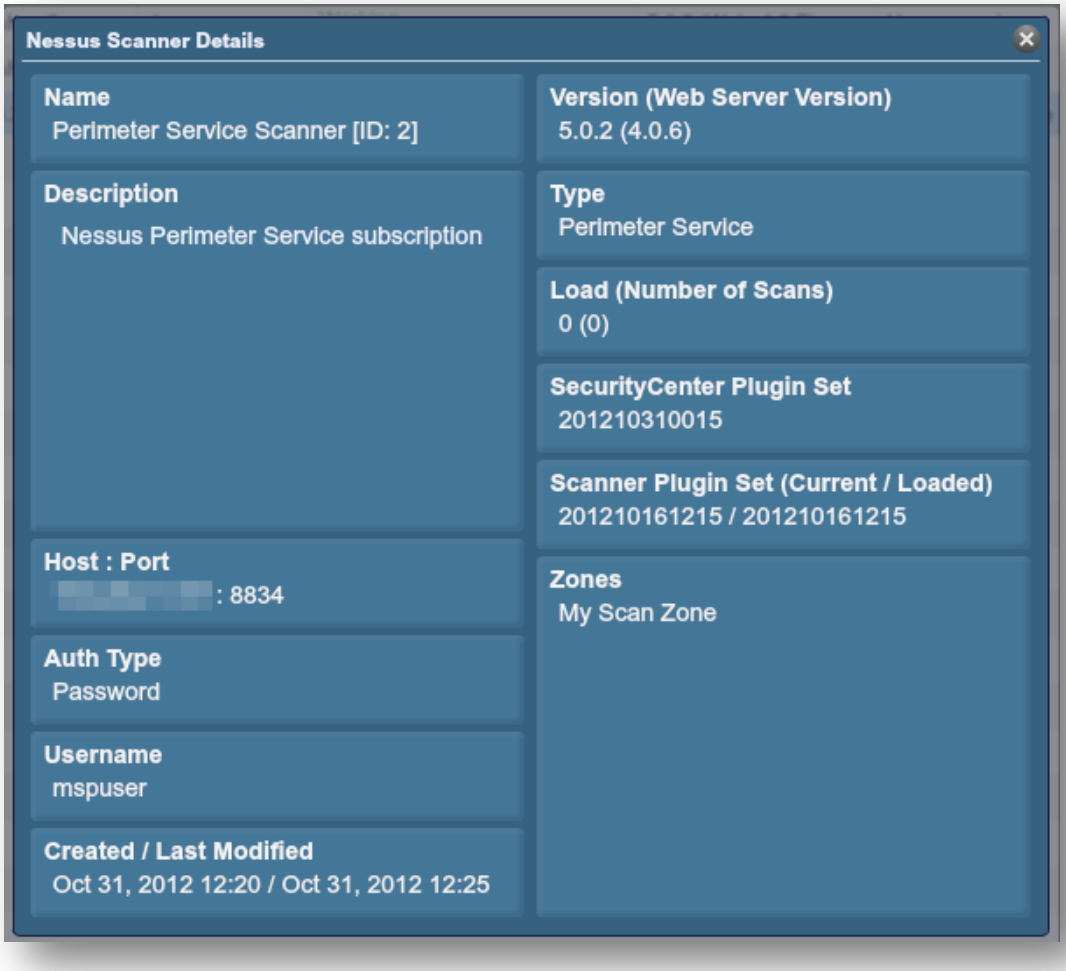
To add a Nessus Perimeter Service scanner to SecurityCenter, a valid and active Nessus Perimeter Service subscription must be used. In SecurityCenter, select the "**Resources**" tab, "**Nessus Scanners**", and then "**Add**":



Enter a name (mandatory) and description (optional) for the Nessus Perimeter Service scanner to be used with SecurityCenter. Enter the web address used for the browser-based version of the Nessus Perimeter Service as "**Host**", with the "**Port**" specified as 443 (HTTPS). Enter a valid Nessus Perimeter Service username and password for authentication and select the zone(s) within SecurityCenter that will use the Nessus Perimeter Service scanner. When finished, click "**Submit**" to add the authorized Nessus Perimeter Service scanner to SecurityCenter. If successful, the Nessus Perimeter Service scanner will be listed under "Nessus Scanners" with a status of "Working":

Note that existing scan reports from the Nessus Perimeter Service are not automatically made available through SecurityCenter, but they can be manually downloaded and imported into SecurityCenter by users with permissions to do so.

Nessus Scanner Details



When the "**Detail**" button is clicked, information about the selected scanner is displayed. The information includes the basic information of name, description, IP address or hostname, port, username used to connect to the scanner, and when the scanner was created and last modified. The Nessus scanner version, web server version, type, and zones it is a part of are also displayed. The number of active scans (load) the server is performing is displayed and updated every 15 minutes, as well as the current SecurityCenter plugin set, the plugin set the Nessus scanner is currently using for scanning, and which plugin set is currently loaded.

The Scanner Plugin Set may show a difference between the "Current" set and the "Loaded" set. This occurs when plugins are updated but the Nessus scanning engine has not been restarted to run the newest plugins.

Scan Zones

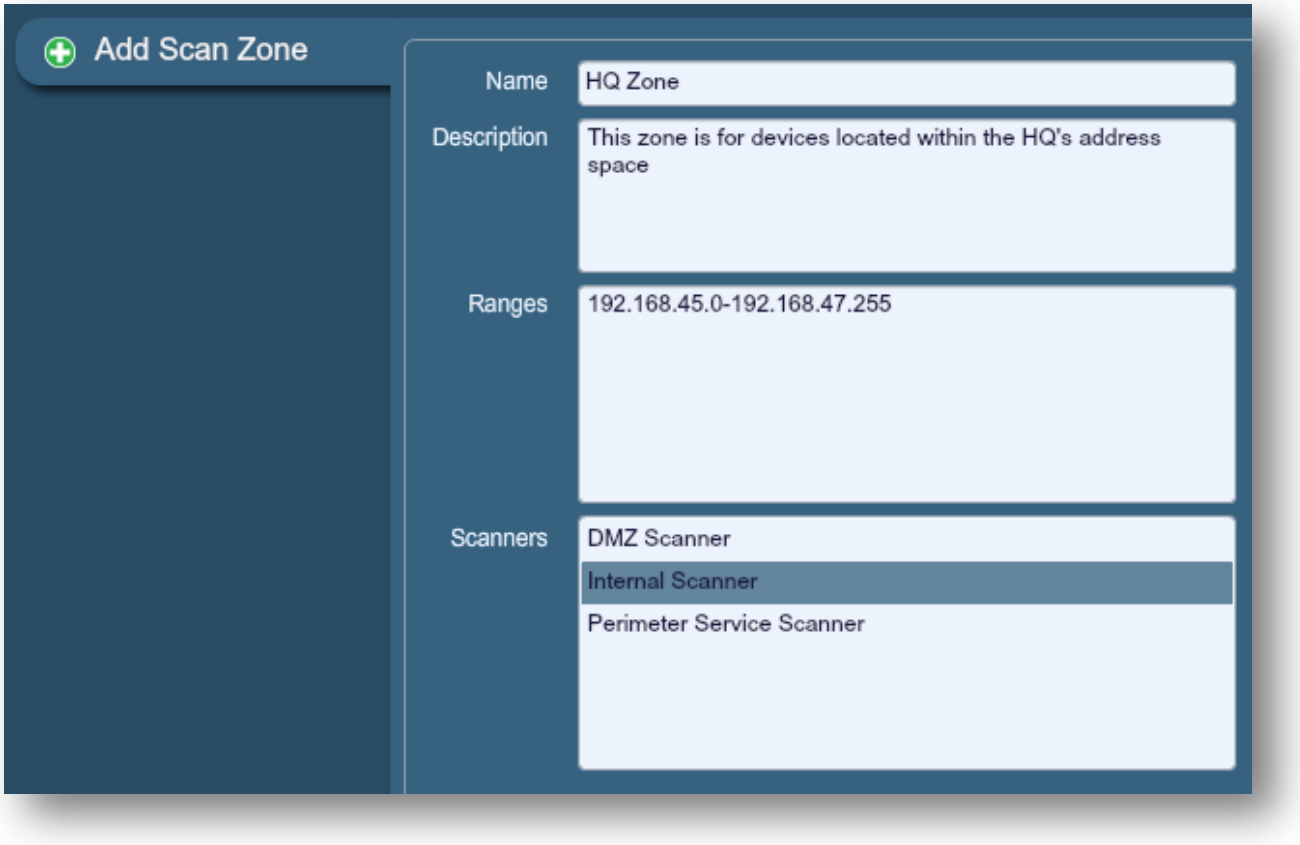
Scan Zones define the IP ranges associated with the scanner along with organizational access. SecurityCenter allows defined Organizations to be configured with two different scan zone modes: "selectable" and "forced". If an Organization is in "selectable" mode, any available zones can be associated with the Organization and made available to users for scanning configuration. If an Organization is in "forced" mode, the selected zone will always be used for every scan performed by users in that Organization.

When in “selectable” mode, at scan time, the zones associated with the Organization and “default” are available to the user. When a scan is configured to use a specific zone in either selectable or forced mode, the zone’s ranges are ignored and any IPs in the managed ranges for that user will be scanned by the Nessus scanners associated with the chosen zone.

When a scan is configured to use the “default” zone, the targets for the scan will be given to scanners in the most appropriate zone available based on the zone’s specified ranges (20K character limit). This facilitates optimal scanning and is very useful if an Organization has devices placed behind a firewall or NAT device and has conflicting RFC 1918 non-internet-routable address space with another Organization. In addition, some Organizations may benefit from the ability to override their default scanner(s) with one(s) from a different zone. This allows an Organization to more easily run internal and external vulnerability scans.

Sometimes forcing a scan to use a “non-ideal” scanner is helpful to analyze the vulnerability stance from a new perspective. For example, setting the default scanner to an external one allows you to see the attack surface from an external attacker’s perspective.

An example Scan Zone configuration screen capture is displayed below:



Passive Vulnerability Scanners

Tenable’s Passive Vulnerability Scanner (PVS) is a patented network discovery and vulnerability analysis software solution, that delivers real-time network profiling and monitoring for continuous assessment of an organization’s security posture in a non-intrusive manner. The PVS monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the PVS behaves like a security motion detector on the network.

PVS records its detected vulnerabilities to a `.nsr` or `.nessus`, file(s), depending on the configuration of the PVS. When used with SecurityCenter 4.6 or IPv6 networks, the PVS scanner must use the `.nessus` file format to record its data. When deployed for operation with SecurityCenter, the PVS uses an agent named the PVS Proxy. This agent is a server that waits for inbound connections from SecurityCenter.

By default, the PVS Proxy listens on port 1243. The port is not hard-coded, and can easily be modified for operation on an alternate port.

SecurityCenter will ask the PVS Proxy for the latest (if any) vulnerability report every 15 minutes. If the PVS is configured to record its passive vulnerability data every six hours, then new passive vulnerability data will only be available to SecurityCenter every six hours.

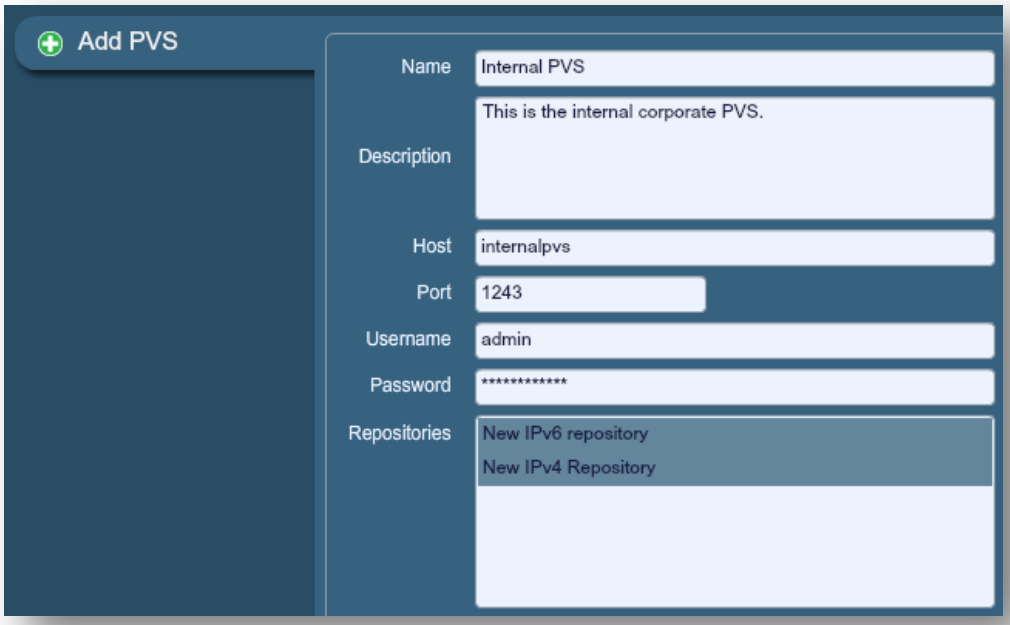
By default, SecurityCenter will check every 24 hours to see if any new passive vulnerability plugins have been downloaded from Tenable and will push them out to each PVS scanner.

The screen capture below shows a listing of working PVS scanners:

To configure one or more of Tenable's PVS servers, under the "**Resources**" tab select "**Passive Scanners**". This will produce a form that lists all configured PVS devices and their current status. Selecting the "**Update Status**" button will initiate a connection from SecurityCenter to obtain and refresh the status of the PVS scanners.

To enable a PVS, add the PVS scanner IP address or hostname, the port its proxy is listening on (1243, by default), its username, password, and then select the repository that will be subscribed to the PVS data. Pressing "Ctrl" or "Shift" on the keyboard when clicking will allow for the selection of multiple repositories to be subscribed to the PVS data. If PVS 3.8 will be reporting IPv4 and IPv6 data, at least two repositories (one for IPv4 and one for IPv6) must be selected. Versions of PVS prior to 3.8 only report IPv4 data.

It is recommended to use passwords that are at least eight characters in length and include a combination of lower and upper-case letters along with non-alphabetic characters.



Log Correlation Engines

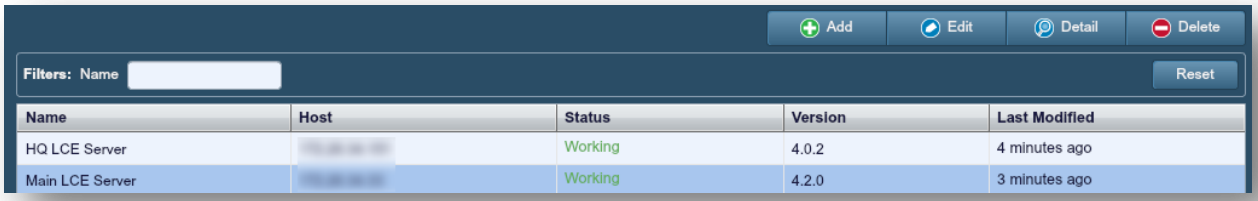
Tenable's Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates, and analyzes event log data from the myriad of devices within the infrastructure. LCE 4.2 also has the ability to analyze logs for vulnerabilities and allows SecurityCenter to retrieve the data. Since LCE is closely integrated with SecurityCenter, log analysis and vulnerability management can be centralized for a complete view of an organization's security posture.

SecurityCenter performs vulnerability, compliance, and event management, but does not directly receive logs or IDS/IPS events. Combining the LCE with SecurityCenter does all of this by processing the events with the LCE and then passing them on to SecurityCenter. Once transferred to SecurityCenter, the logs are aggregated further and made available for analysis and reporting.

LCE version 4.2 is required for complete compatibility. Using a mixture of LCE 3.x and 4.x will result in most of the newer features in version 4.x to be unused.

More than one Log Correlation Engine can be configured to work with SecurityCenter.

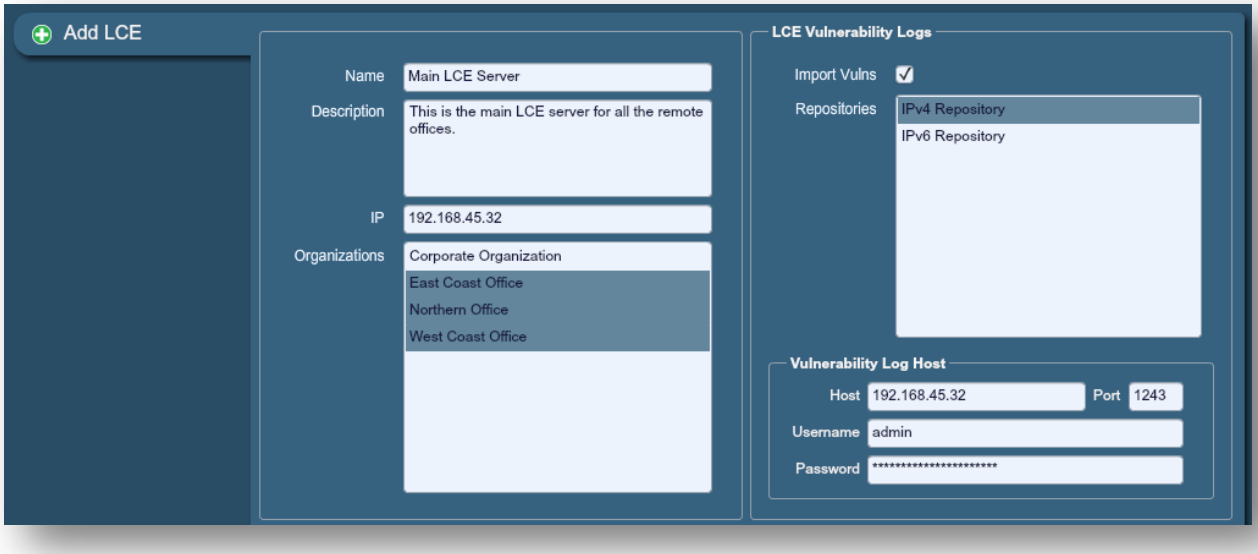
To configure LCE servers, select "**Log Correlation Engines**" under the "**Resources**" tab. A screen will be displayed similar to the following:



Click "**Add**" to display the dialog in the screen capture below. Default viewable fields include **Name**, **Description**, **Host**, **Organizations**, and an unchecked checkbox for **Import Vulns**. When the **Import Vulns** option is selected, additional fields become available for **Repositories** selection and **Vulnerability Log Host** settings.

LCE server 4.2 will also generate vulnerability logs. Enabling the **Import Vulns** option allows SecurityCenter to collect and import the vulnerability information from the LCE 4.2 server. The **Repositories** area defines the repositories to receive the data. The **Vulnerability Log Host** section configures the IP address, port, username, and password to log into the LCE 4.2 server to retrieve the vulnerability information. The username and password are set when configuring the LCE server and is typically different than the system username and password used to configure the SSH key exchange described in the next section.

After submitting the information, the remote LCE login prompt will be displayed so that the SecurityCenter can authenticate with the LCE server. This is a one-time process to exchange SSH keys for secure communication between SecurityCenter and LCE. If remote root or root equivalent user login is prohibited in your environment, refer to Appendix 2 for instructions on how to manually configure the LCE server using SSH key authentication.



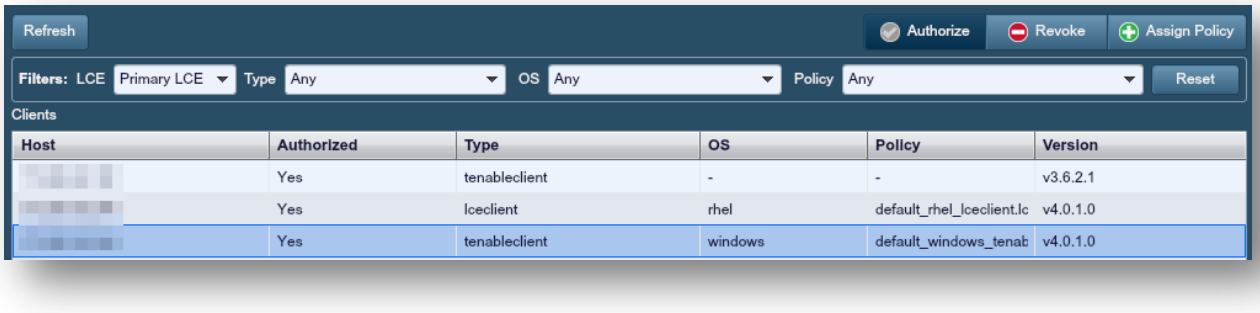
If organizational policy prohibits remote root login, a manual key exchange process can be used. See Appendix 2: Manual LCE Key Exchange for detailed guidance.

Table 9 – LCE Options

Option	Description
Name	Name used to describe the Log Correlation Engine.
Description	Descriptive text for the Log Correlation Engine.
IP	IP address of the Log Correlation Engine.
Organizations	Determines which Organizations will be able to access data from the configured Log Correlation Engine.
Import Vulns	When enabled, allows Event vulnerability data to be retrieved from the configured LCE 4.2 server.
Repositories	Select the appropriate SecurityCenter repository(ies) to store the imported LCE data.
Vulnerability Log Host	Configures the **Host**, **Port**, **Username**, and **Password** settings to retrieve Event vulnerability reports. The **Host** setting is populated by default with the same IP address as the LCE IP setting. It may be adjusted manually as needed. If using the Event vulnerability logs feature on an LCE server and a PVS server on the same host IP, ensure that the PVS-proxy port and Event vulnerability log host reporter-port are configured for different ports.

Log Correlation Engine Clients

Beginning in LCE 4.0, the LCE server has the ability to manage configuration files for LCE 4.x clients remotely from the command line. SecurityCenter 4.6 introduces the ability to manage the configuration files for LCE 4.x clients via a graphical interface.



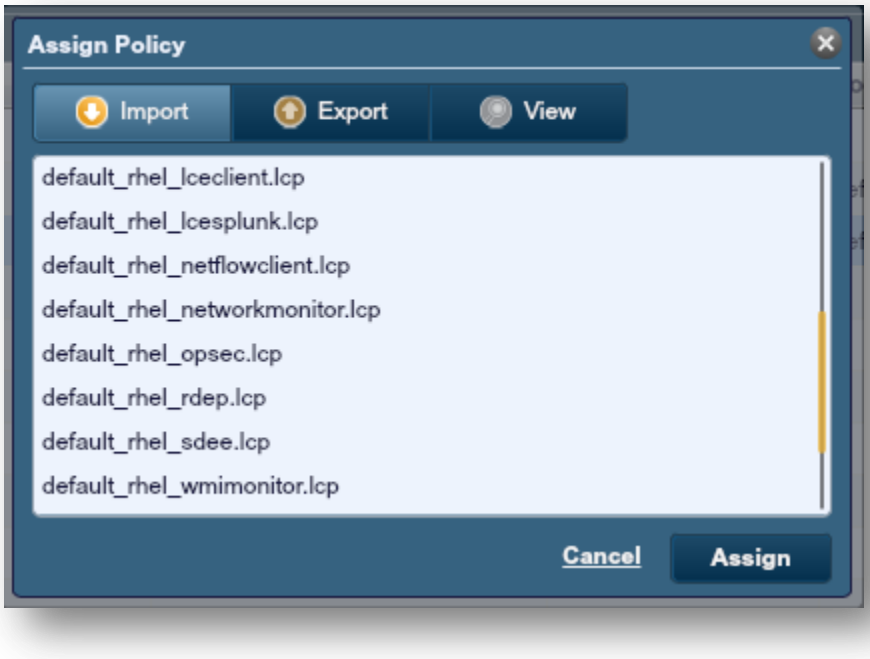
The default view for the LCE Clients page displays all of the available clients for the selected LCE server in the "**Filters**" section, and may be changed using the drop-down box. Using the "**Type**", "**OS**", and "**Policy**" filters, the displayed clients may be narrowed down by a mix of criteria based on the client type, host OS, and assigned client policy file.

LCE Client versions 4.0 and higher display information in the table including their host address, authorization status, client type, host OS, assigned policy file, and client version. These clients may all have their configuration files managed from SecurityCenter.

Note that configured clients prior to version 4.x are displayed on the list without OS and policy information. However, these clients cannot have their policy files centrally managed from SecurityCenter.

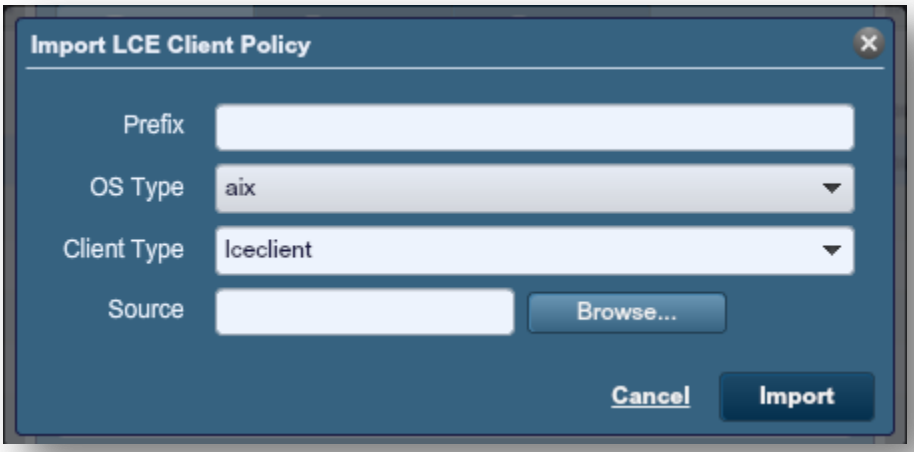
LCE Clients are initially configured to send their data to a particular LCE server, but must be authorized by the LCE sever for the server to accept the data. The client's authorization status is displayed in the "**Authorized**" column as "Yes" or "No". This may be toggled by selecting the client from the list and clicking either the "**Authorize**" or "**Revoke**" button as appropriate.

Each client must have a policy assigned to it that specifies the appropriate data to send. The currently assigned policy is displayed in the "**Policy**" column. To change the assigned policy, select the client to modify from the list, and click the "**Assign Policy**" button.



The Assign Policy window allows you to import, export, view LCE Client policy files, and assign polices to clients. Policies with the prefix of "default" are created and supplied by Tenable primarily as examples that can be customized for local use.

Note: The default policies that are supplied by Tenable may be modified and updated on the LCE server during plugin updates. It is recommended that the default policies be saved to a different name if they are modified for local use.



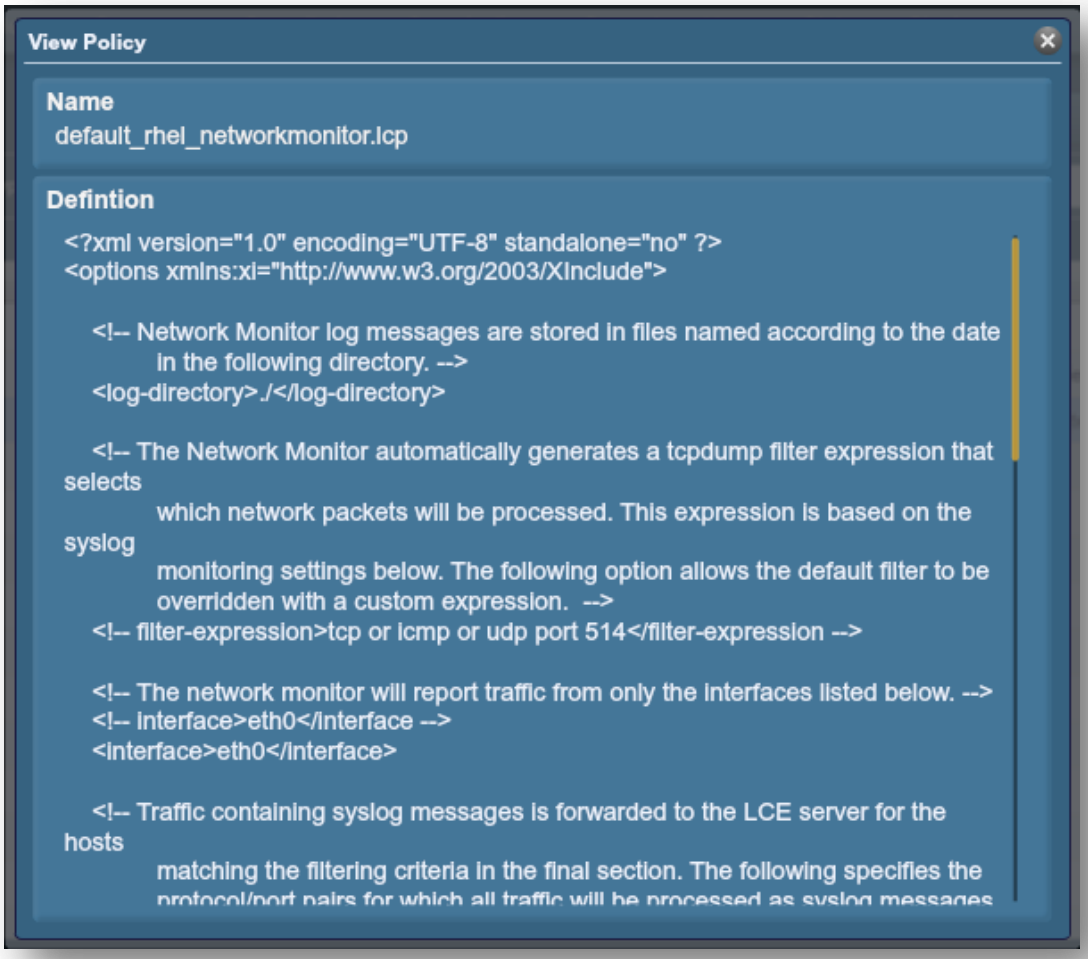
“Import” allows customized LCE Client policy files to be added to the LCE server and made available for use. The prefix field is appended to the beginning of the file name and is used to offer a description of the function or use of the policy file. The OS Type is used in the file name to easily identify the OS for which the policy is designed. The Client Type indicates the LCE Client for which the policy is written. The Source field is used to select and upload the custom policy file to the LCE server.

The “default” prefix is only designed to be used by policies supplied by Tenable. Using “default” as a prefix for custom policy files may lead to them being overwritten or manipulated in undesired ways.

Once the fields are set appropriately, clicking the **“Import**” button will upload the new client policy to the LCE server and make it available for use.

Selecting a policy and clicking the “**Export**” button will allow the policy to be saved to a local drive. The format of the file is XML and may be edited with standard text or XML editors.

Selecting a policy and clicking the “**View**” button displays the policy in a window within SecurityCenter. The information cannot be edited from within this window.



Once a policy has been selected for use with the chosen client, click the "**Assign**" button to associate the policy file with the client. When the client makes its next connection to the LCE server, it will acquire its new policy file, apply it to its configuration, and restart with the new settings.

For more information on creating LCE Client Policy files, please see the LCE Client Guide available on the Tenable Support Portal.

Data Management

Repositories

A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. SecurityCenter integrates repositories of vulnerability data that are shared as needed among users and organizations based on manager-defined assets. The use of repositories allows for scalable and configurable data storage for organizations. Repository data can also be shared between multiple SecurityCenters. Repositories are configured by the administrative user and made available to the Organization Head to assign to users as needed.

When creating SecurityCenter repositories, LCE event source IP ranges must be included along with the vulnerability IP ranges or the event data and event vulnerabilities will not be accessible from the SecurityCenter UI.

There are three types of repositories: “Local”, “Remote”, and “Offline”. Local repositories are active repositories of SecurityCenter data collected via scanners attached to the local SecurityCenter. Remote repositories contain IP address and vulnerability information obtained via network synchronization with a second (remote) SecurityCenter. Offline repositories enable SecurityCenter to obtain repository data via manual export/import from a remote SecurityCenter that is not network-accessible. The screen capture below shows several configured repositories. Note that the “Type” column only displays when there are repositories other than Local.

As shown in the screen capture above, hover the cursor over the “Total Active IPs” graphic at the bottom of the screen to view currently used IPs, total IP license count, and IPs remaining.

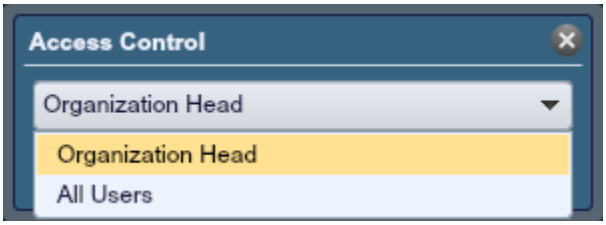
Repository data collected from a remote or offline repository is static and used solely for reporting purposes.

Click the “**Add**” button to add a new repository. The sections below contain options for adding each of the three types of repositories.

Local Repository

This is the default repository type. Data stored in local repositories can be shared between Organizations and includes the full range of event and vulnerability metadata. The table below describes configurable fields for a local repository:

Table 10 – Local Repository Options

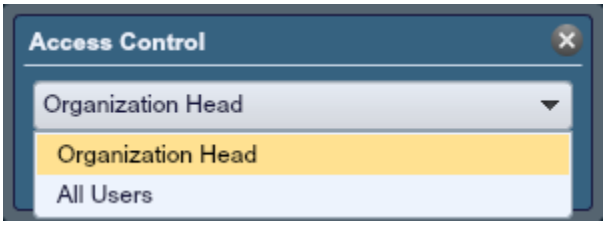
Option	Description
Name	The repository name.
Description	Descriptive text for the repository.
Type	Local
IP Version	Determines if the repository will store IPv4 or IPv6 results. SecurityCenter repositories cannot store a mix of IPv4 and IPv6 addresses.
Trending	If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the `.nessus` data for vulnerability trending purposes. This option is useful in cases where tracking data changes is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.
Generate Nessus File	Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day), and Monthly (Date).
Download Format	Allows for selecting between the Nessus v1 and v2 formats for the generated Nessus file. When IPv6 data is used, the v2 format must be selected.
IP Ranges	Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).
LCE Correlation	Log Correlation Engine servers that will receive the vulnerability correlation information from this repository.
Organizations	Organizations that have access to the vulnerability data within the repository. Within the “Organizations” section, click the green key icon for access control options. Access is available for the “Organization Head” user or for “All Users” within the Organization (affects existing users only). 

Remote Repository

Remote repositories are useful because they allow separate SecurityCenters to share repository data via a SSH session. The table below describes configurable fields for a remote repository:

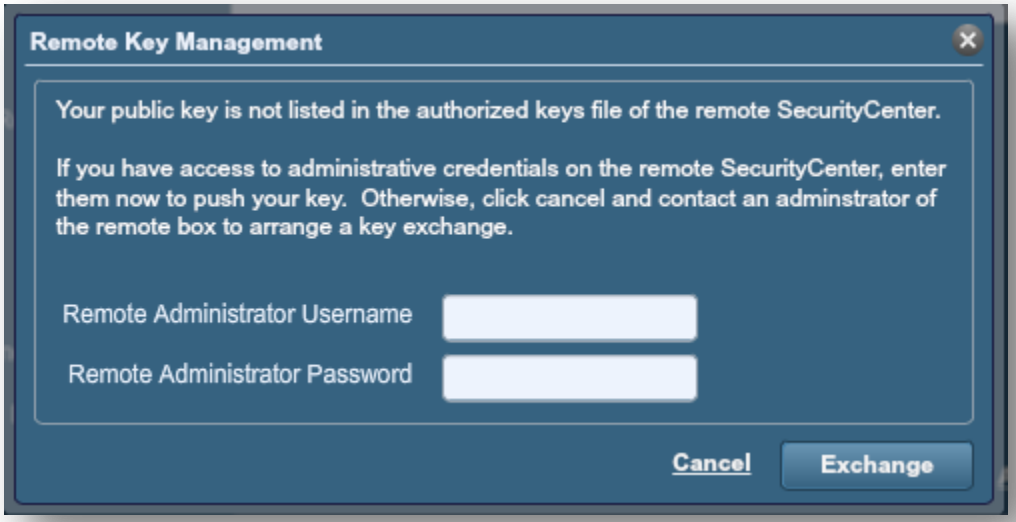
Table 11 – Remote Repository Options

Option	Description
Name	The repository name.
Description	Descriptive text for the repository.
Type	Remote
Remote Repository	Host to synchronize with to obtain the repository data. After entering the hostname or IP address of the remote SecurityCenter, click the "Retrieve Repositories" link to enter an admin username and password for the SecurityCenter to exchange the SSH keys. Once completed, a list of available repositories will be populated.
Repository	Remote repository to collect IP address(es) and vulnerability data from. This is a drop-down list of the available repository names available on the remote SecurityCenter.
IP Version	For a remote repository, this setting is determined by the remote repository and cannot be selected.
Trending	If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the `.nessus` data for vulnerability trending purposes. This option is useful in cases where tracking data changes is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.
Generate Nessus File	Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day), and Monthly (Date). The `.nessus` files generated by this process can be imported into Nessus scanners or any third-party tool that accepts the `.nessus` format as required. This option is not related to the "Sync Schedule" below, which relates to automating the synchronization of vulnerability data between SecurityCenters.
Download Format	Allows for selecting between the Nessus v1 and v2 formats for the generated Nessus file. When IPv6 data is used, the v2 format must be selected.
Sync Schedule	Frequency with which the local and remote repositories are synchronized. Synchronization options include: "Never", "Daily", "Weekly", "Monthly (Date)", and "Monthly (Day)". Click the "Time Zone" link to ensure the Sync Schedule time is being performed at the correct local time.
IP Ranges	Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).
Organizations	Organizations that have access to the vulnerability data within the repository. Within the "Organizations" section, click the green key icon for access control options. Access is available for the "Organization Head" user or for "All Users" within the Organization (affects existing users only). For existing repository edits, an additional option labeled "Existing Users" is available. This option leaves the current user access intact. Click "**Submit**" to apply the changes.

To share data, enter the IP address of the remote SecurityCenter in the “Host” field and click “**Retrieve Repositories**”.

If a key for the current SecurityCenter has not been added to the remote SecurityCenter key list, the retrieve process will prompt for the SecurityCenter admin credentials of the remote host.


Remote Key Management
Your public key is not listed in the authorized keys file of the remote SecurityCenter.
If you have access to administrative credentials on the remote SecurityCenter, enter them now to push your key. Otherwise, click cancel and contact an adminstrator of the remote box to arrange a key exchange.
Remote Administrator Username
Remote Administrator Password
Cancel
Exchange

If the key authentication is not configured (**System** -> **Keys**), a prompt for the administrator username and password for the remote host will be displayed. Repository IP addresses and vulnerability/event data is then retrieved from the remote SecurityCenter for use in the new one.

Offline Repository

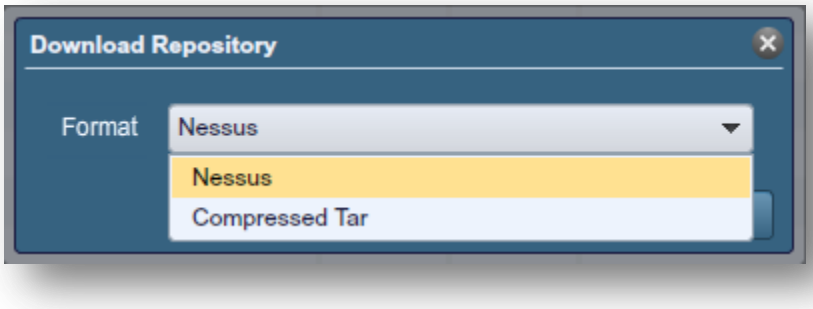
Offline repositories are similar to remote repositories with the exception that data is synchronized manually using an archive file (`.tar.gz`) and not via network transmission. The table below describes configurable fields for an offline repository:

Table 12 – Offline Repository Options

Option	Description
Name	The repository name
Description	Descriptive text for the repository

Type	Offline
IP Version	Determines if the repository will store IPv4 or IPv6 results. SecurityCenter repositories cannot store a mix of IPv4 and IPv6 addresses.
Trending	If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the .nessus data for vulnerability trending purposes. This option is particularly useful in cases where trending is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.
Generate Nessus File	Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day), and Monthly (Date). The `.nessus` files generated by this process can be imported into Nessus scanners or any third-party tool that accepts the `.nessus` format as required.
Download Format	Allows for selecting between the Nessus v1 and v2 formats for the generated Nessus file. When IPv6 data is used, the v2 format must be selected.
IP Ranges	Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).
Organizations	Organizations that have access to the vulnerability data within the repository. Within the “Organizations” section, click the green key icon for access control options. Access is available for the “Organization Head” user or for “All Users” within the Organization (affects existing users only). For existing repository edits, an additional option labeled “Existing Users” is available. This option leaves the current user access intact. Click “**Submit**” to apply the changes.

To initiate offline repository synchronization, first download the repository archive from an existing repository by clicking on the “**Download**” link. You may download the archive as a Nessus or Compressed Tar (`.tar.gz`) formatted file.

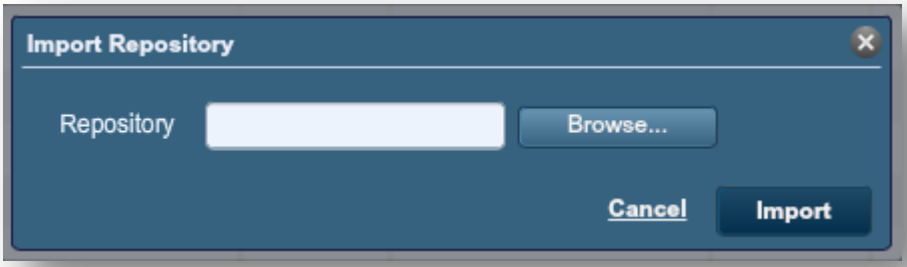


Depending on browser choice, the option to open or save the Nessus or Compressed Tar file is presented. It is recommended that the file be saved at this time.

Depending on the size of the repository database, this file can be quite large. It is important to save the file to a location with plenty of free disk space.

When importing the repository archive, the default maximum file import size is 160MB. This is specified by the "post_max_size" directive in `/opt/sc4/support/etc/php.ini`. If larger file uploads are required, increase the default value.

To load the repository archive to the offline repository, copy it to a location where the offline repository is accessible via the SecurityCenter GUI, open the "**Repositories**" page, highlight the offline repository and click "**Sync**".

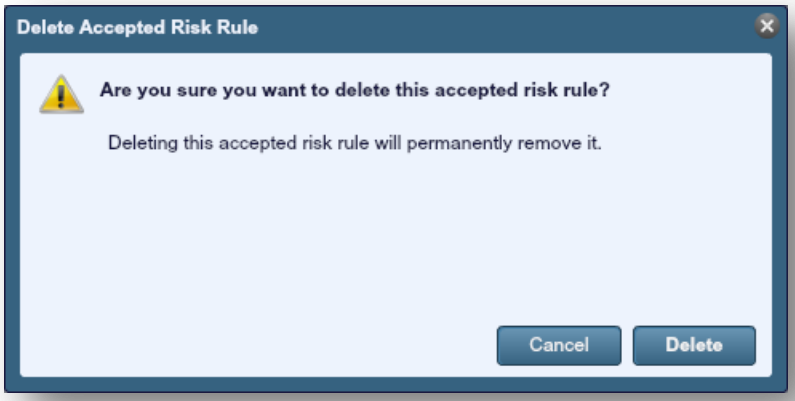


Browse for the repository archive and click "**Submit**" to load the offline repository archive file.

Accept Risk Rules

Any non-admin user has the ability to accept a vulnerability risk by adding an "**Accept Risk Rule**". Adding a rule moves vulnerabilities from the unfiltered cumulative database view. These vulnerabilities are not deleted, but only display in the cumulative database vulnerability view if the "Accepted Risk" filter option is checked. Once a risk has been accepted, the admin user can view the details of and delete the accept rules associated with the risk if they deem that the risk is still valid. This is accomplished by clicking on "**Repositories**" and then "**Accept Risk Rules**". From there a list of available rules is displayed for the selected Plugin ID, Repository, and Organization combination. Choose "All" for Repository and "Any" for Organization if plugin IDs are to be accepted across these boundaries. This is especially useful in setups where hundreds of repositories or organizations have been configured and the same accept risk rule must be applied globally.

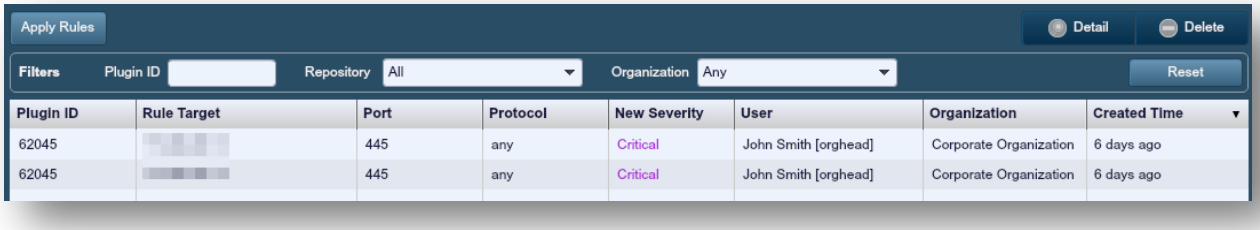
Select the rule to be removed and click "**Detail**" to view the highlighted "Accept Risk Rule". To remove the rule, click "**Delete**" and a confirmation dialog is displayed that confirms if you really wish to delete the accepted risk rule:


Delete Accepted Risk Rule
Are you sure you want to delete this accepted risk rule?
Deleting this accepted risk rule will permanently remove it.
Cancel
Delete

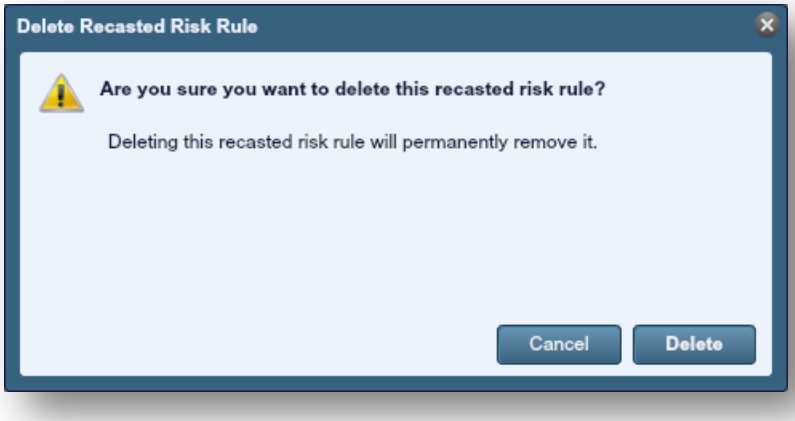
After clicking "**Delete**", click the "**Apply Rules**" button in the top left for the changes to take effect. Once completed, any vulnerabilities that had been modified by the accept risk rule are displayed unfiltered in the cumulative database.

Recast Risk Rules

Similar to "Accept Risk Rules", "**Recast Risk Rules**" are rules that have been recast to a different risk level by a non-admin user. The admin user can display and delete these rules if desired. As with "Accept Risk Rules", rules can be applied for a single plugin ID against a single repository/organization combination or globally. A screen capture of example "Recast Risk Rules" is shown below:



To view the rule details, click "**Detail**" to view the highlighted "Recast Risk Rule". To remove the rule, click "**Delete**". A confirmation dialog is displayed and confirms that you really wish to delete the recasted risk rule:


Delete Recasted Risk Rule
Are you sure you want to delete this recasted risk rule?
Deleting this recasted risk rule will permanently remove it.
Cancel
Delete

After clicking “**Delete**”, click the “**Apply Rules**” button in the top left for the changes to take effect. Once completed, any vulnerabilities that had been modified by the recasted risk rule are returned to their original state.

User Management

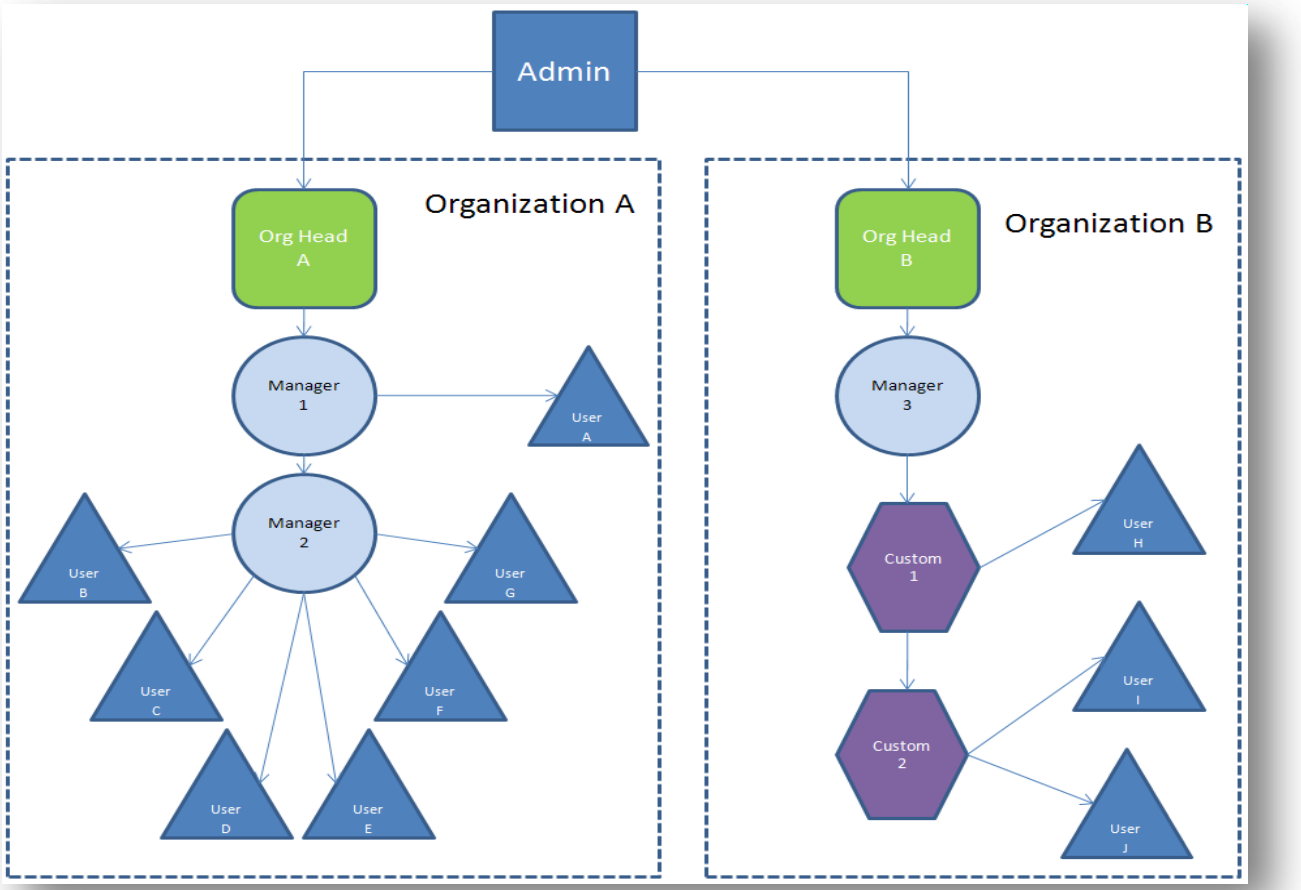
Organizations

Many of the concepts in this section such as zones, multiple organizations, and repositories apply only to SecurityCenter and not the LCE Manager.

An Organization is defined as a set of distinct Users. These Users are assigned repositories and “zones” within one or more specified IP networks. “Users” refers to any non-administrator login account on SecurityCenter. “Zone” means that each Organization is made up of the systems within one or more IP networks.

Multiple Organizations can share the same repository, and the vulnerability data associated with the overlapping ranges will be shared between each Organization. Conversely, Organizations can be configured with their own discrete repositories to facilitate situations where data must be kept confidential between different organizational units.

The Organization is managed primarily by the Administrator and Organization Head users. The Administrator is responsible for Organization and Organization Head creation and maintenance. Users within the Organization are created by the Organization Head user or any user with the “Manage Users” permissions. User management is strictly hierarchical. For example, consider the diagram below:

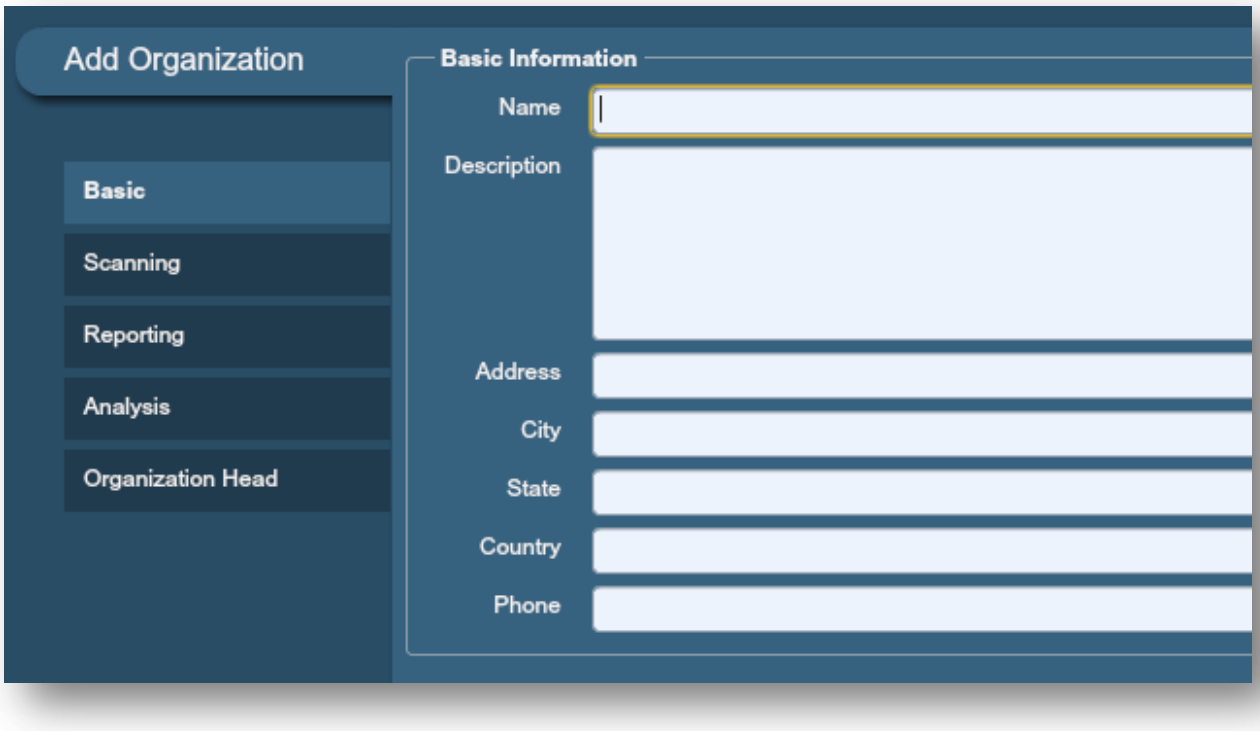


In Organization A, the Org Head user has control over all Users and Managers in Organization A. Manager 1 similarly has control over all Users and Managers (except the Org Head user). Manager 2, however, only has control over Users B through G since User A and Manager 1 are not in their hierarchy.

In Organization B, Manager 3 has control over all Organizational Users except for the Org Head user. We have created two users with custom roles. These custom roles have the “Manage Users” role and subsequently were able to create Users H through J. Custom 1 has control over Custom 2 along with all Users; however, Custom 2 only has control over Users I and J.

It is important to consider these concepts when working with the built-in roles and creating custom ones as they relate to your organizational structure.

Creation of an Organization is a multi-step process. The screen capture below contains five tabs: Basic, Scanning, Reporting, Analysis, and Organization Head.



The table below describes options available during the creation of an Organization:

Table 13 – Basic Options

Option	Description
Basic Information	
Name	Organization name (Required)
Description	Descriptive text for the Organization.

Address	Organization address
City	Organization city
State	Organization state
Country	Organization country
Phone	Organizational telephone number

The following table describes the options available on the “Scanning” tab.

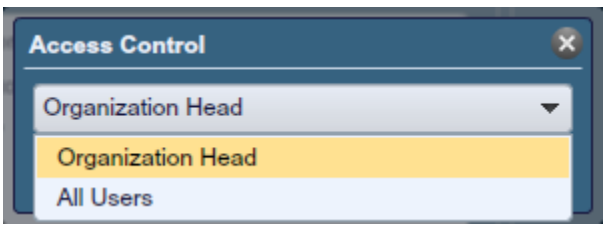
Table 14 – Scanning Options

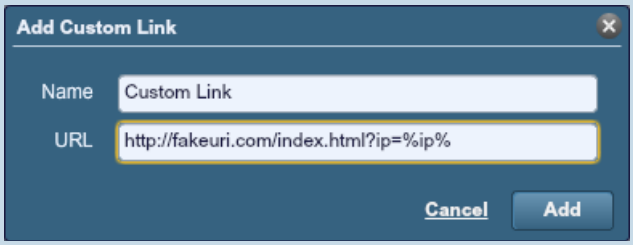
Option	Description
Restricted Scan Ranges	IP range(s) that the scanner will not scan (20K character limit).
Zone Selection	Forced or Selectable. When in “selectable” mode, the user can select from the list of associated zones and choose one or more zones, or set the zone to default. When in “forced” mode, one zone will always be used for every scan.
Zones	Scan zones available to Nessus scanners.

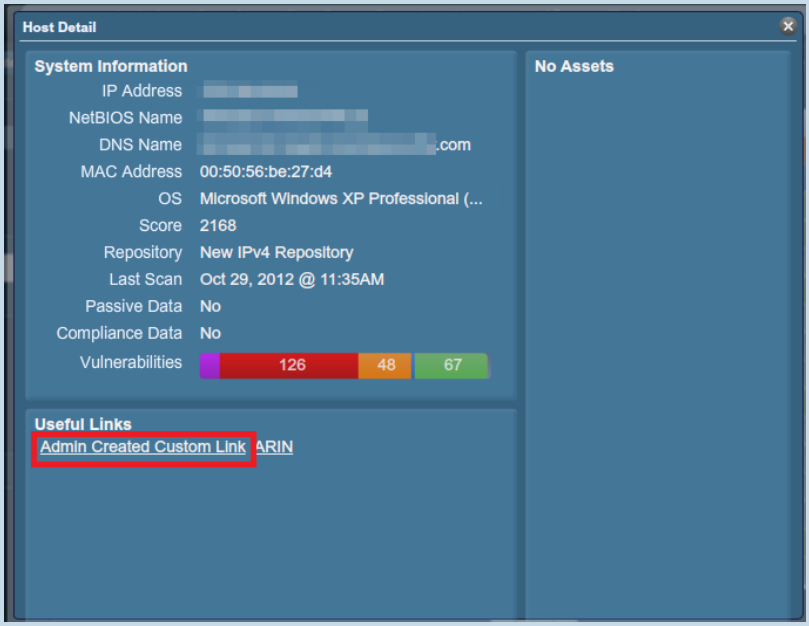
The “Reporting” tab allows you to select Publishing Sites that will be available to the Organization. Single or multiple sites may be selected.

The following table describes the options available on the “Analysis” tab.

Table 15 – Analysis Options

Option	Description
Accessible LCEs	LCE(s) to which this Organization has access.
Accessible Repositories	Repositories to which the Organization will have access. Next to each repository checkbox is a key image that is used to determine repository access. Clicking a key image brings up the dialog below:  Choose “All Users” if all users within the Organization will have access to the selected

	repository. Likewise, choose “Organization Head” if only the Organization Head will have access. Choose “Existing Users” to maintain the current user permissions (applicable when editing an existing Organization).
Vulnerability Weights	
Low	The vulnerability weighting to apply to “Low” criticality vulnerabilities for scoring purposes. (Default: 1)
Medium	The vulnerability weighting to apply to “Medium” criticality vulnerabilities for scoring purposes. (Default: 3)
High	The vulnerability weighting to apply to “High” criticality vulnerabilities for scoring purposes. (Default: 10)
Critical	The vulnerability weighting to apply to “Critical” criticality vulnerabilities for scoring purposes.(Default: 40) Prior to SecurityCenter 4.4 and Nessus 5, critical vulnerabilities were only available after recasting a risk. Nessus 5 now reports some vulnerabilities as a “Critical” severity level.
Custom IP Information Links	
Add New Custom Link	 This tool allows the user to add a custom link within the host vulnerability details. Specify the desired link name and URI. For example: http://fakeuri.dom/index.htm?ip=%ip% The “%ip%” reference is a variable that inserts the IP address of the current host into the specified URI. In the example above, if the IP address of the host is 192.168.0.1, the link URI would be: http://fakeuri.dom/index.htm?ip=192.168.0.1 This link is displayed under “Useful Links” from the Host Detail view (**Vulnerabilities** -> **IP Summary** -> **Host Detail**). Access the “Host Detail” view by clicking on the IP Address link on the IP Summary page.



This link is useful for organizations that want to reference an internal web page with IP specific information. For example, an analyst may need more information about a specific host available in another application. This link could be configured to that external application to provide further information about the host in question, which could assist with vulnerability or event analysis.

The table below describes options required during the creation of an Organization Head:

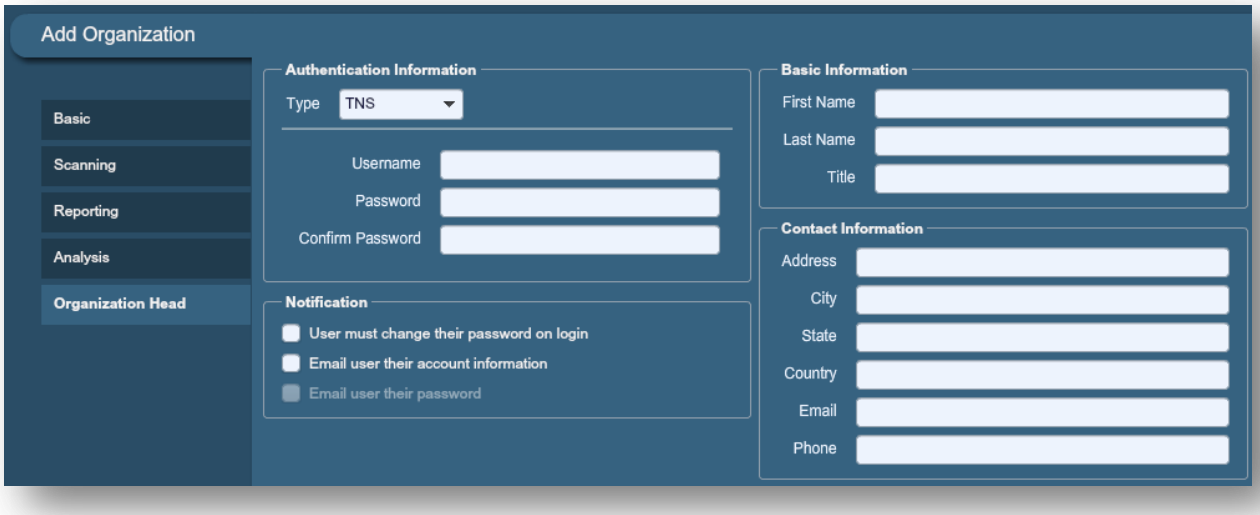


Table 16 – Organization Head Options

Option	Description
Lock	This command button provides the administrator the ability to lock or unlock the Organization Head user. When a user is locked, they are prevented from logging into

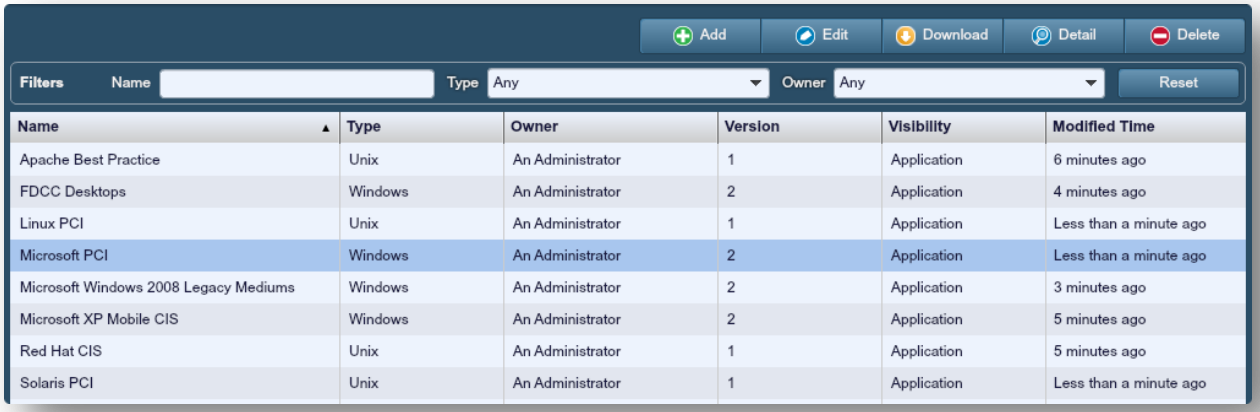
	their account until an administrator unlocks them. This option is only available once the Organization Head user is created.
Authentication Information	
Type – TNS	
Username	Unique organizational login name The username value is case-sensitive.
Password and Confirm Password	Organization Head password creation fields
Type – LDAP	
Search String	This is the LDAP search string to use to narrow down user searches. Proper format is: “attribute=<filter text>”. Wildcards are permitted and the field accepts up to 1024 characters. For Example: sAMAccountName=* mail=a* displayName=C*
Users	This box contains a list of users obtained from the configured LDAP server that match the Search String above.
Username	User that is selected from the list of users above.
Notification	
Email user their account information	Email the Organization Head their account information using the supplied email address.
Email user their password	Email the Organization Head their password using the supplied email address. (TNS Authentication only)
User must change their password on login	Force the Organization Head to change their password on next login. (TNS Authentication only)
Basic/Contact Information	
Name, Title, Address Information, Email, Phone	Contact information for the Organization Head can be entered here.

Support

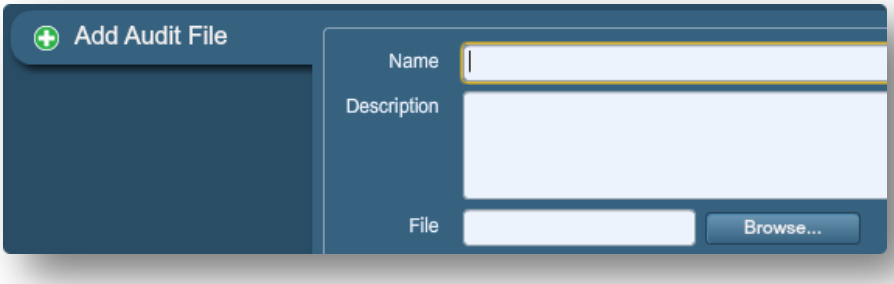
Audit Files

The Nessus vulnerability scanner includes the ability to perform compliance audits of numerous platforms including databases, Cisco, Unix, and Windows configurations as well as sensitive data discovery based on regex contained in "`.audit`" files. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed.

Tenable provides a wide range of audit files and new ones are easy to write. These audit files are maintained on the Tenable Support Portal for users who wish to perform compliance and configuration auditing. The screen capture below contains a listing of an audit file page with PCI DSS and CIS-based audits.



Audit files are added, edited, downloaded, viewed, and deleted from this web interface. Clicking "**Add**" displays the following "Add Audit File" dialog screen:



Available fields include:

Table 17 – Audit File Fields

Option	Description
Name	A descriptive name assigned to the audit file (not necessarily the actual file name)
Description	Descriptive text about the audit file

File	An interface that allows you to browse your local system or file shares for the audit file

Once an audit file has been uploaded, it can be referenced from within scan policies for enhanced security policy auditing. For more information about SecurityCenter compliance auditing and audit files, refer to the Nessus Compliance Checks document located at https://support.tenable.com.

Credentials

Credentials are reusable objects that facilitate scan target login. Credentials created by the admin user are available to all Organizations, while those created by Organizational users are only available to the applicable Organization. Various types of credentials can be configured for use in scan policies. Credentials can be shared between users for scanning purposes and allow the user to scan a remote host without actually knowing the login credentials of the host. Available credential types include:

- Windows – Nessus has vulnerability checks that can use a Microsoft Windows domain account to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been applied. To use this feature, enter the Username, Password, and Domain in the text boxes.

Using a non-administrator account will greatly affect the quality of the scan results. Often it makes sense to create a special Nessus user with administrative privileges that is used solely for scheduled scanning.

- SSH (password with optional privilege escalation and key-based) – SSH credentials are used to obtain local information from remote Linux, Unix, and Cisco IOS systems for patch auditing or compliance checks. There is a field for entering the SSH username for the account that will perform the checks on the target system, along with either the SSH password or the SSH public key and private key pair. There is also a field for entering the passphrase for the SSH key, if it is required. In case of invalid or expired SSH keys use the “Clear” button to remove the current SSH keys.

  The most effective credentialed scans are those with “root” privileges (“enable” privileges for Cisco IOS). Since many sites do not permit a remote login as “root”, a Nessus user account can invoke a variety of privilege escalation options including: “su”, “sudo”, “su+sudo”, “DirectAuthorize (dzdo)”, “PowerBroker (pbrun)”, and “Cisco Enable”.

PowerBroker (pbrun), from BeyondTrust and DirectAuthorize (dzdo), from Centrify, are proprietary root task delegation methods for Unix and Linux systems.

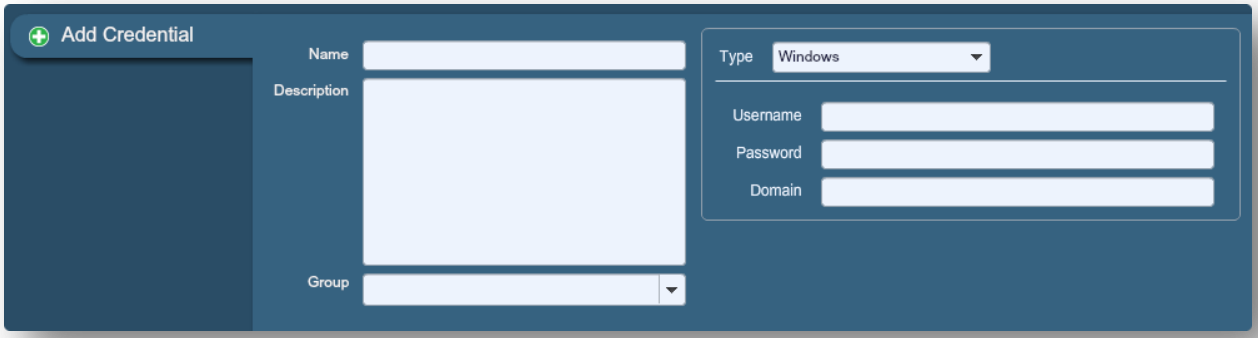
Scans run using “su+sudo” allow the user to scan with a non-privileged account and then switch to a user with “sudo” privileges on the remote host. This is important for locations where remote privileged login is prohibited.

Scans run using “sudo” vs. the root user do not always return the same results because of the different environmental variables applied to the “sudo” user and other subtle differences. Please refer to the “sudo” man pages or the following web page for more information: http://www.gratisoft.us/sudo/man/sudo.html#Security%20Notes

To direct the Nessus scanner to use privilege escalation, click the drop-down menu labeled “Privilege Escalation” and select the appropriate option for your target system. Enter the escalation information in the provided box.

- SNMP community string – Enter the SNMP community string used for authentication.
- Kerberos – The Kerberos IP, Port, Protocol, and Realm are available for this type of authentication.

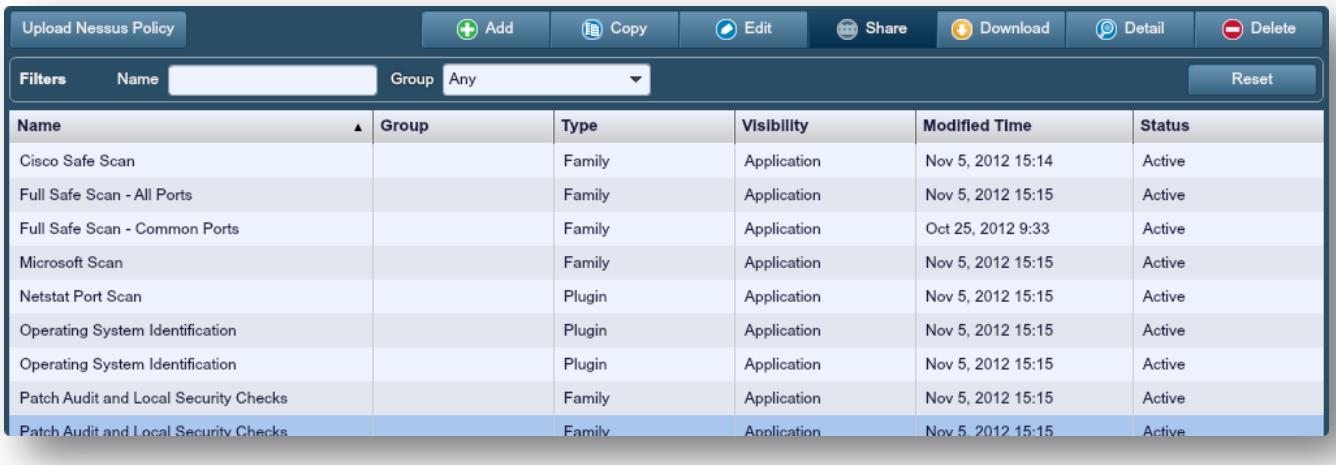
An example Windows credential with options is displayed below:



Some aspects of credential options are based on Nessus plugins, therefore, specific credential options may differ from the descriptions documented here.

Scan Policies

The scan policy contains plugin settings and advanced directives used during the course of the Nessus scan. Scan policies created by the admin user are available to all organizations configured on the SecurityCenter. Click "**Support**" and then "**Scan Policies**" to display a listing of all currently available policies. Scan Policies created using Nessus may be uploaded with the **Upload Nessus Policy** button on the upper-left side of the window. This will open a window enabling the selection of the policy file and addition of a name, description, and group. Audit files and credentials from the original policy are not exported and copied with the policy file. Tabs at the upper-right portion of this page provide the ability to **Add**, **Copy**, **Edit**, **Share**, **Detail** (view details of), and **Delete** existing policies.

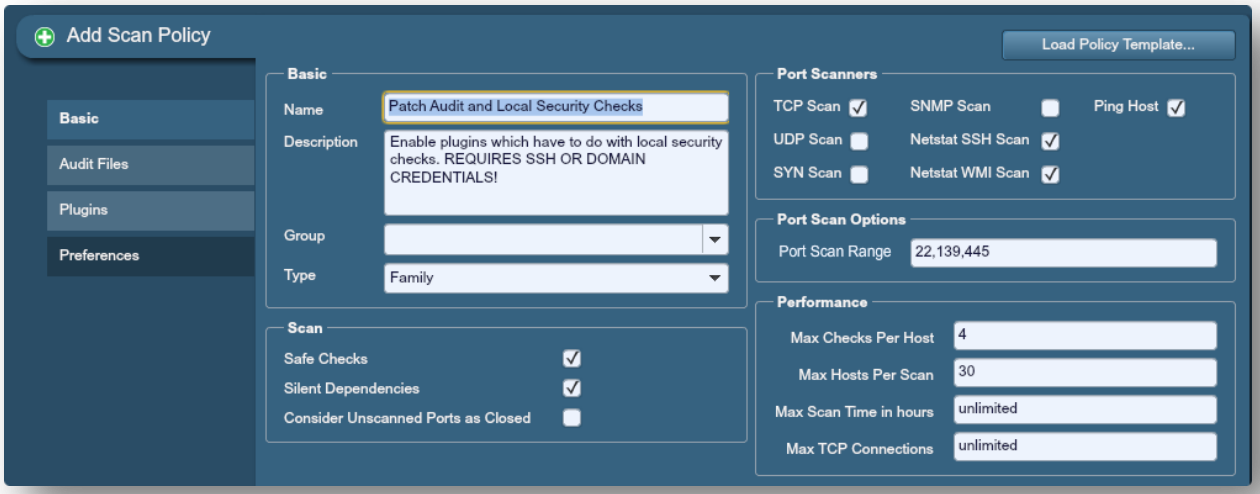


Name	Group	Type	Visibility	Modified Time	Status
Cisco Safe Scan		Family	Application	Nov 5, 2012 15:14	Active
Full Safe Scan - All Ports		Family	Application	Nov 5, 2012 15:15	Active
Full Safe Scan - Common Ports		Family	Application	Oct 25, 2012 9:33	Active
Microsoft Scan		Family	Application	Nov 5, 2012 15:15	Active
Netstat Port Scan		Plugin	Application	Nov 5, 2012 15:15	Active
Operating System Identification		Plugin	Application	Nov 5, 2012 15:15	Active
Operating System Identification		Plugin	Application	Nov 5, 2012 15:15	Active
Patch Audit and Local Security Checks		Family	Application	Nov 5, 2012 15:15	Active
Patch Audit and Local Security Checks		Family	Application	Nov 5, 2012 15:15	Active

Add a Scan Policy

Clicking "**Add**" opens the following screen, which is used to configure the new scan policy. Four tabs are displayed including:

- Basic
- Audit Files
- Plugins
- Preferences



Basic

The "**Basic**" tab contains basic scan policy settings and allows the user to load a predefined scan policy template. The "**Load Policy Template**" option is a command button located in the upper right-hand corner of the "**Basic**" tab page and allows the user to load scan policy options based on a variety of predefined scan policy templates. Available templates include: "Web Safe Scan", "FTP Safe Scan", "SMTP Safe Scan", "Cisco Safe Scan", "Full Safe Scan – All Ports", "Full Safe Scan – Common Ports", "Microsoft Scan", "PCI DSS Scan", "Topology Scan", "Peer-To-Peer Scan", "Virus Check Scan", "Operating System Identification", "Patch Audit and Local Security Checks", and "Netstat Port Scan". These templates use optimized plugin and configuration settings for their specified scan type.

The tables below contain detailed descriptions of options available on each of the five frames displayed under the "**Basic**" tab:

Table 18 – Basic Options

Option	Description
Name	Unique policy name
Description	Policy description (optional)
Group	Policy group name (optional)

Type	Family or Plugin. If “Family” is chosen, then when plugin updates occur, new plugins will automatically be enabled for plugin families that are enabled. If “Plugin” is enabled, only the currently enabled plugins are enabled. New plugins must be manually enabled by the user. This is beneficial where strict control over new plugins is required. Changing from “Family” to “Plugin”, or vice-versa, clears all currently enabled plugins. Please make a note of all enabled plugins before changing this option so that they can be enabled afterwards.

The “**Scan**” frame controls basic scan options for the scan:

Table 19 – Scan Options

Option	Description
Safe Checks	Nessus can attempt to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When “Safe Checks” is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.
Silent Dependencies	If this option is checked, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, uncheck the box.
Consider Unscanned Ports as Closed	With this setting enabled, ports that are not enumerated by the port scan will not be tested. For example, scanning ports 21, 22, and 23 will only test those ports and not any other port.

The “**Port Scanners**” frame controls which methods of port scanning should be enabled for the scan:

Table 20 – Port Scanner Options

Option	Description
TCP Scan	Use Nessus’ built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features. On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.
UDP Scan	This option engages Nessus’ built-in UDP scanner to identify open UDP ports on the targets. UDP is a “stateless” protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable. Utilizing the UDP scanner will noticeably increase scanning time.
SYN Scan	Use Nessus’ built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits

	for SYN-ACK reply, and then determines port state based on a reply – or lack of.
SNMP Scan	Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under "Preferences", this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Netstat SSH Scan	This option uses **`netstat`** to check for open ports on the target host. It relies on the **`netstat`** command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.
Netstat WMI Scan	This option uses **`netstat`** to check for open ports from the local machine. It relies on the **`netstat`** command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials.
Ping Host	This option enables the pinging of remote hosts to determine if they are alive. This option is not recommended when scanning between virtual hosts on the same system.

The "**Port Scan Options**" frame directs the scanner to target a specific range of ports. The following values are allowed for the "Port Scan Range" option:

Table 21 – Values for Port Scan Options

Value	Description
"default"	Using the keyword "default", Nessus will scan approximately 4,789 common ports (found in the **`nessus-services`** file).
Custom List	A custom range of ports can be selected by using a comma delimited list of ports or port ranges. For example, "21,23,25,80,110" or "1-1024,8080,9000-9200" are allowed. Specifying "1-65535" will scan all ports.

The range specified for a port scan will be applied to both IPv4 and IPv6 addresses, as well as TCP and UDP scans.

The "**Performance**" frame provides two options that control how many scans will be launched. These options are perhaps the most important when configuring a scan as they have the biggest impact on scan times and network activity.

Table 22 – Performance Options

Option	Description
Max Checks Per Host	This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.
Max Hosts Per Scan	This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For

	example, if the Max Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.
Max Scan Time in hours	This setting limits the length of time a scan is allowed to run. If a scan reaches this limit, the unscanned targets are captured in a new "rollover" scan that can be run manually or scheduled at a later time.
Max TCP Connections	This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.

Audit Files

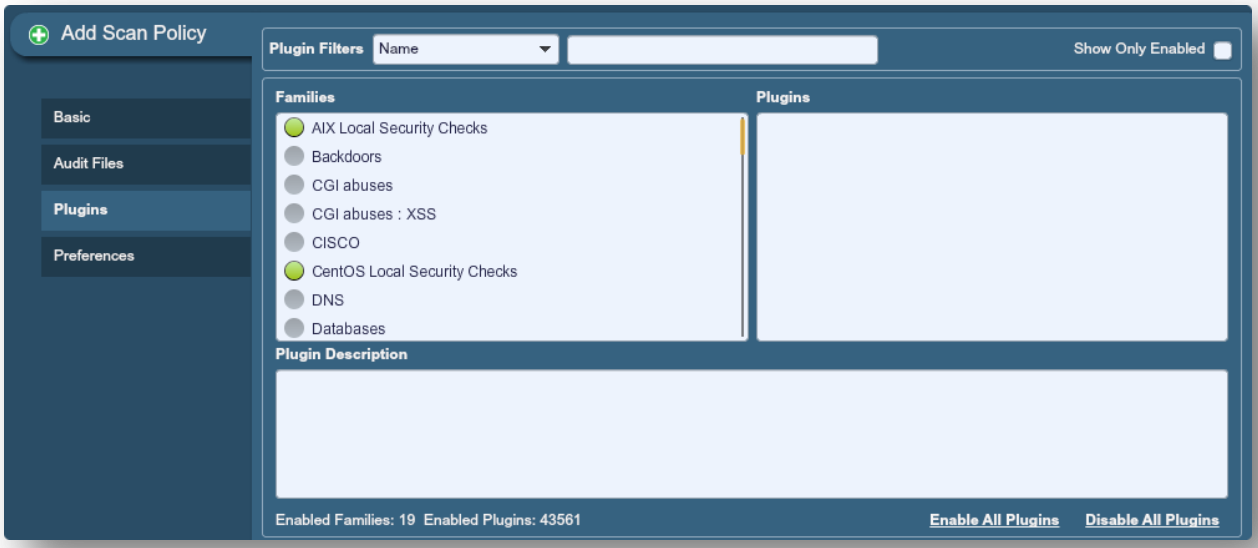
The **Audit Files** tab contains two options related to Nessus compliance scans. Note that you must at least name the scan from the "Basic" frame to be able to open the "Audit Files" tab.

Table 23 – Audit File Options

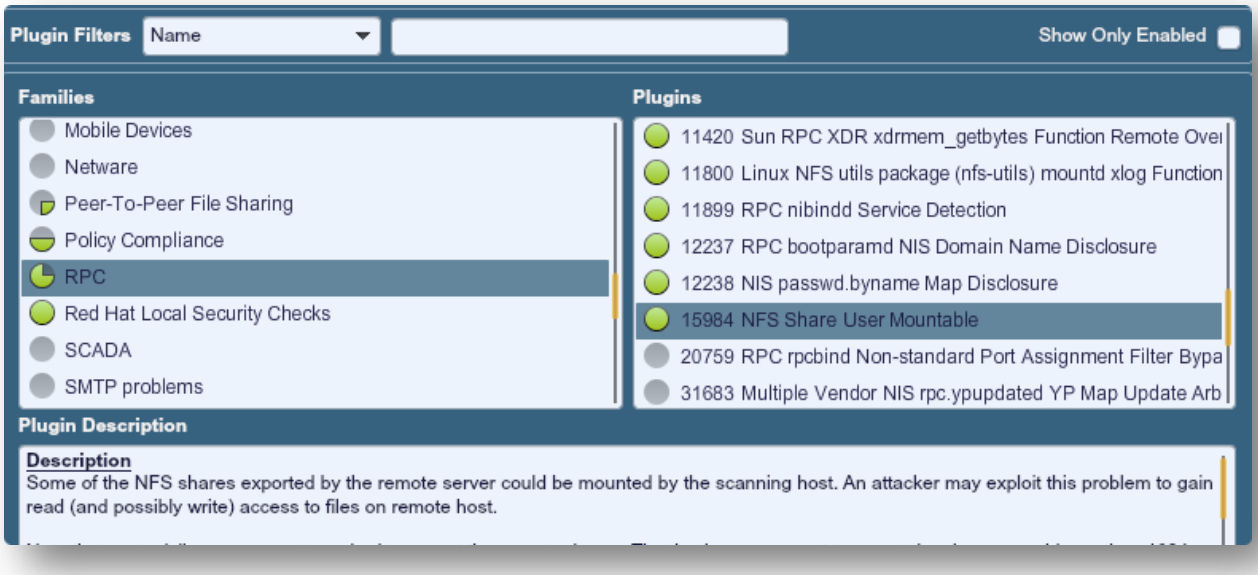
Option	Description
Select Audit File	Tenable provides a variety of `.audit` files that provide a template check for compliance audits against various established standards, such as the Center for Internet Security (CIS) benchmarks, healthcare industry standards (HIPAA), Payment Card Industry (PCI) requirements, and many more. To perform a compliance check, you must have the ability to perform authenticated Unix/Linux and/or Windows local checks.
Perform PCI DSS Analysis	The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services, and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is in use by many e-commerce vendors who accept and store credit card data. Tenable provides three plugins to all SecurityCenter users that automate the process of performing a PCI DSS audit. These plugins are: • PCI DSS compliance: tests requirements • PCI DSS compliance: passed • PCI DSS compliance These plugins evaluate the results of your scan and the actual configuration of your scan to determine if the target server is PCI compliant. The plugins do not perform actual scanning; they just look at the results from other plugins. To activate the PCI DSS plugins, simply check the box labeled "Perform PCI DSS Analysis" from the "Compliance" screen. It is important to note that a secure infrastructure is achieved through a fusion of people, processes, and technology. Tenable's solutions provide the technology to aid in compliance requirements and are intended to be used in conjunction with a comprehensive security strategy. Please consult with your organization's Audit and Compliance group for guidance and directives specific to your organization.

Plugins

The “**Plugins**” tab gives the user the option to customize which plugins are used during the policy’s Nessus scan.



Clicking the circle next to a plugin family allows you to enable or disable the entire family. The circles next to the name under Families will show green when some or all of the plugins for that family are enabled. The green will show as full if all the plugins are selected, or ¼, ½, or ¾ full when some plugins in the family are selected, where the circle’s green fill approximates the number of plugins selected.


Plugin Filters
Name
Show Only Enabled
Families
Plugins
Mobile Devices
Netware
Peer-To-Peer File Sharing
Policy Compliance
RPC
Red Hat Local Security Checks
SCADA
SMTP problems
11420 Sun RPC XDR xdrmem_getbytes Function Remote Ove
11800 Linux NFS utils package (nfs-utils) mountd xlog Function
11899 RPC nibindd Service Detection
12237 RPC bootparamd NIS Domain Name Disclosure
12238 NIS passwd.byname Map Disclosure
15984 NFS Share User Mountable
20759 RPC rpcbind Non-standard Port Assignment Filter Bypa
31683 Multiple Vendor NIS rpc.ypupdated YP Map Update Arb
Plugin Description
Description
Some of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may exploit this problem to gain read (and possibly write) access to files on remote host.

Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in the “Plugin Description” pane will also show solution information, additional references if available, and the CVSSv2 score that provides a basic risk rating.

When a policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin feed update, they will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family will automatically be disabled as well.

The “Denial of Service” family contains some plugins that could cause outages on network hosts if the “Safe Checks” option is not enabled, but does contain some useful checks that will not cause any harm. The “Denial of Service” family can be used in conjunction with “Safe Checks” to ensure that any potentially dangerous plugins are not run. However, it is recommended that the “Denial of Service” family not be used on a production network.

The following table describes options that will assist you in selecting plugins.

Table 24 – Plugin Options

Option	Description
Plugin Filters	Display plugins based on selected parameters including Name, ID, Family, CVE, BID, and Cross-References). Select the parameter you wish to search and type in some text to look for and hit Enter.
Show Only Enabled	Select this checkbox to only show currently enabled plugins.
Enable All Plugins	Enable all available plugins.
Disable All Plugins	Disable all available plugins.

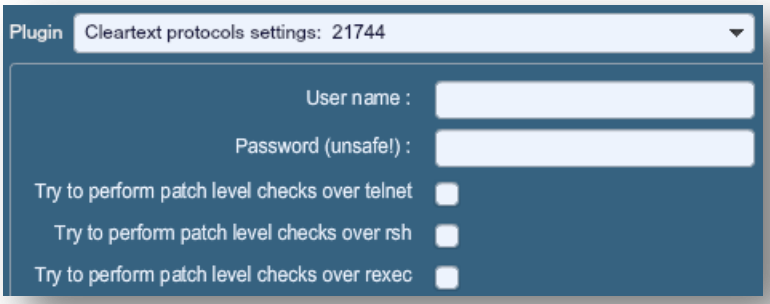
Preferences

The “**Preferences**” tab includes means for granular control over scan settings. Selecting an item from the drop-down menu will display further configuration items for the selected category.

Note that this is a dynamic list of configuration options that is dependent on the plugin feed, audit policies, and additional functionality to which the connected Nessus scanner has access. This list may also change as plugins are added or modified.

The **Cisco IOS Compliance Checks** (plugin 46689) options determine the Cisco IOS configuration file to audit. The available options are Saved, Running, or Startup. Only one type of configuration file may be selected.

If a secure method of performing credentialed checks is not available, users can force Nessus to attempt to perform checks over insecure protocols by configuring the **Cleartext protocols settings** (plugin 21744) drop-down menu item. The cleartext protocols supported for this option are **telnet**, **rsh**, and **rexec**. The “unsafe!” warning serves as a reminder that the information is being sent across the network in an unencrypted manner.


Plugin
Cleartext protocols settings: 21744
User name :
Password (unsafe!) :
Try to perform patch level checks over telnet
Try to perform patch level checks over rsh
Try to perform patch level checks over rexec

The **Database settings** (plugin 33815) options apply to database compliance audits and are used to specify the type of database to be tested, relevant settings, and credentials:

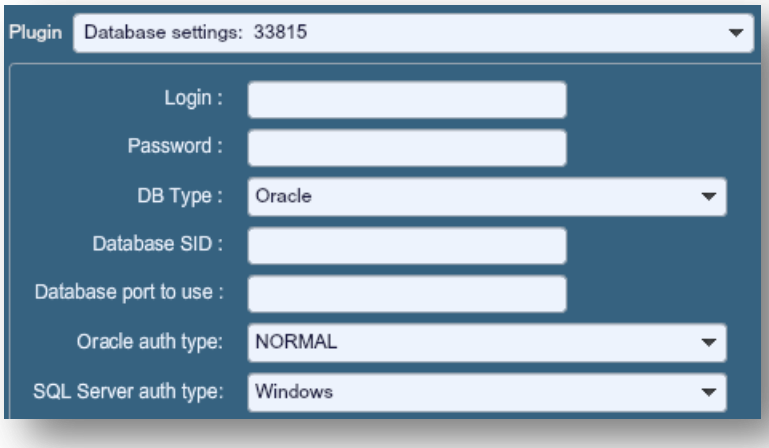


Table 25 – Database Settings

Option	Description
Login	The username for the database.
Password	The password for the supplied username.
DB Type	Oracle, SQL Server, MySQL, DB2, Informix/DRDA, and PostgreSQL are supported.
Database SID	Database system ID to audit (Oracle only).
Database port to use	Port the database listens on. This is useful where the database is configured to listen on a non-standard port. If this field is not specified, the default port for the chosen database is used: • Oracle: 1521 • MySQL: 3306

	• SQL Server: 1433 • Informix: 1526 • DB2: 50000
Oracle auth type	NORMAL, SYSOPER, and SYSDBA are supported. Depending on the privileges required by the `.audit` commands, enhanced privileges such as “SYSOPER” or “SYSDBA” may be required. In most cases, however, the “NORMAL” auth type will suffice.
SQL Server auth type	Windows or SQL are supported.

Do not scan fragile devices (plugin 22481) instructs the Nessus scanner not to scan network printers or Novell Netware hosts if unselected. Since both of these technologies are more prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.

Global variable settings (plugin 12288) contains a wide variety of configuration options for the Nessus server.

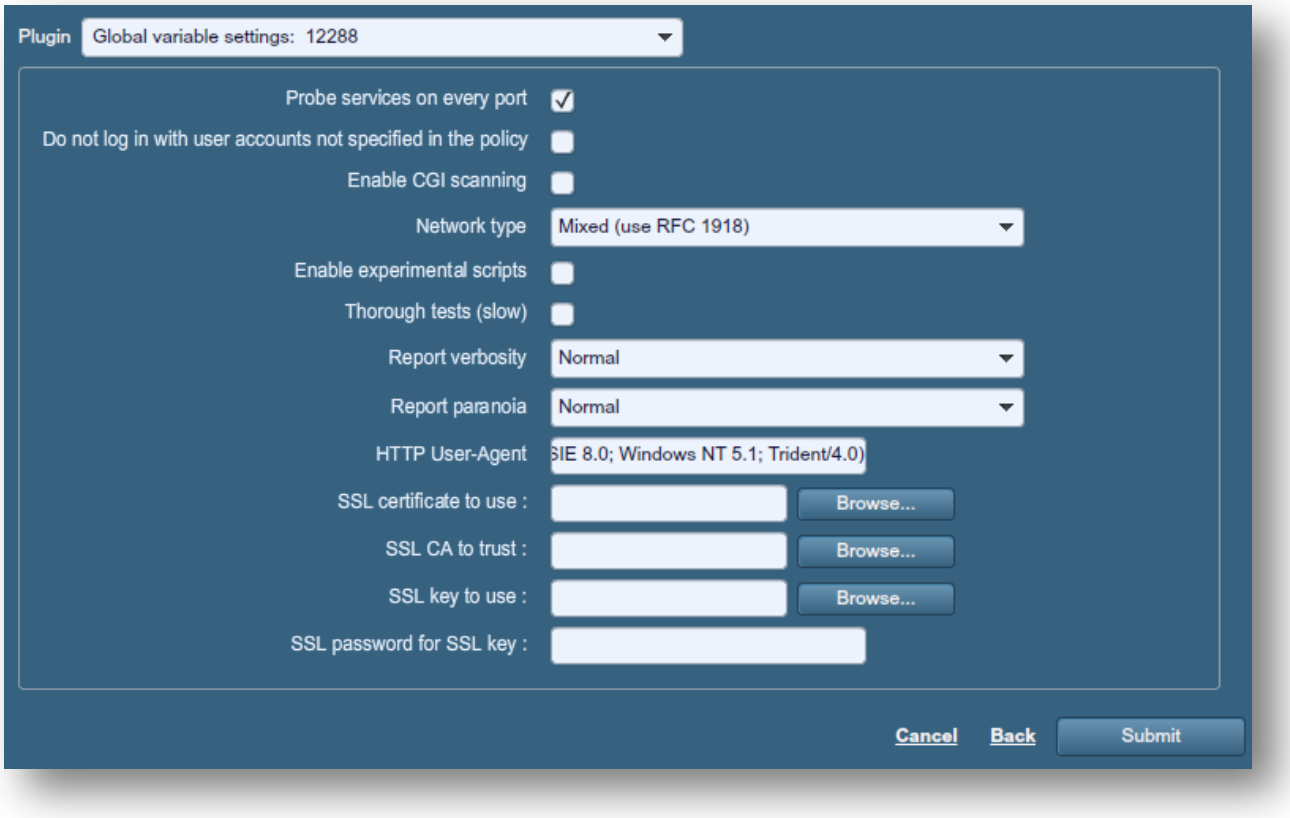


Table 26 – Global Variable Settings

Option	Description
Probe services on every port	Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.

Do not log in with user accounts not specified in the policy	Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.
Enable CGI scanning	Activates CGI checking. Disabling this option will greatly speed up the audit of a local network. This option must be enabled in conjunction with the web application testing plugin for a full web audit to occur.
Network type	Allows you to specify if you are using public routable IPs, private non-internet routable IPs or a mix of these. Select "Mixed" if you are using RFC 1918 addresses and there are multiple routers within your network.
Enable experimental scripts	Causes plugins that are considered experimental to be used in the scan. Do not enable this setting while scanning a production network. Tenable does not release scripts flagged "experimental" in either plugin feed.
Thorough tests (slow)	Causes various plugins to "work harder". For example, when looking through SMB file shares, a plugin can analyze 3 levels deep instead of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially having better audit results. For more information about "thorough tests" see this blog entry.
Report verbosity	A higher setting will provide more information in the report.
Report paranoia	In some cases, Nessus cannot remotely determine whether a flaw is present or not. If the report paranoia is set to "**Paranoid (more false alarms)**" then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of "**Avoid false alarm**" will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. The default option ("**Normal**") is a middle ground between these two settings.
HTTP User-Agent	Specifies which type of web browser Nessus will impersonate while scanning.
SSL certificate to use	Allows Nessus to use a client side SSL certificate for communicating with a remote host.
SSL CA to trust	Specifies a Certificate Authority (CA) that Nessus will trust.
SSL key to use	Specifies a local SSL key to use for communicating with the remote host.
SSL password for SSL key	The password for managing the SSL key specified.

HTTP cookies import (plugin 42893) facilitates web application testing. Nessus can import HTTP cookies from another piece of software (web browser, web proxy, etc.) with this setting. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.

The **HTTP login page** (plugin 11149) settings provide control over where authenticated testing of a custom web-based application begins. See this blog entry for more details about configuring web applications that require authentication.

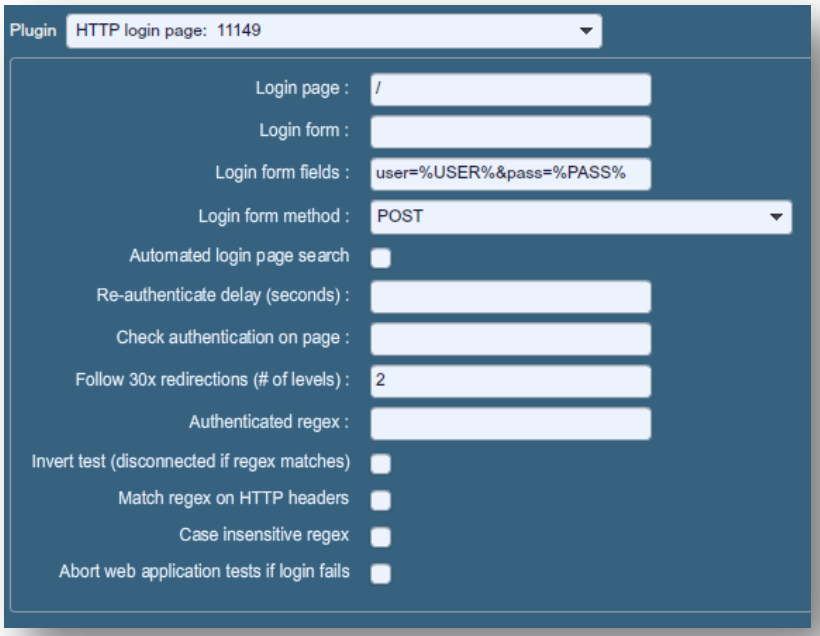


Table 27 – HTTP Login Page Settings

Option	Description
Login page	The base URL to the login page of the application.
Login form	The “action” parameter for the form method. For example, the login form for <form method="POST" name="auth_form" action="/login.php"> would be “/login.php”. This option is not required if the “Automated login page search” option specified below is used.
Login form fields	Specify the authentication parameters (e.g., `login=%USER%&password=%PASS%`). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the “Login configurations” drop-down menu. This option is not required if the “Automated login page search” option specified below is used.
Login form method	Specify POST or GET based on the login form requirements. This option is not required if the “Automated login page search” option specified below is used.

Automated login page search	Gives Nessus the option to parse the login page for form options and attempt to log in based on detected fields. This option works in conjunction with the HTTP cookies import (plugin 42893) to simplify form-based authentication. If more than one form is available on a web page (uncommon), use the manual login form parameters specified above instead.
Re-authenticate delay (seconds)	The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.
Check authentication on page	The URL of a protected web page that requires authentication, to better assist Nessus in determining authentication status.
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.
Authenticated regex	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as “Authentication successful!”
Invert test (disconnected if regex matches)	A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., “Authentication failed!”).
Match regex on HTTP headers	Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.
Case insensitive regex	The regex searches are case sensitive by default. This instructs Nessus to ignore case.
Abort web application tests if login fails	If authentication fails to the web page, further actions by the plugin will be halted.

IBM iSeries Credentials (plugin 57861) accepts a login name and password for authentication to IBM’s iSeries systems.

The **ICCP/COTP TSAP Addressing** (plugin 23812) menu deals specifically with SCADA checks. It determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to “8” by default.

LDAP ‘Domain Admins’ Group Membership Enumeration (plugin 58038) allows for the entry of an LDAP user and password to be used to attempt to enumerate the members of the ‘Domain Admins’ group on an LDAP server search base, which is identified using the LDAP Crafted Search Request Server Information Disclosure plugin (25701). The Max Results setting limits the enumeration of users to the number entered (1,000 by default).

Login configurations (plugin 10870) allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3 or IMAP. By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied here will be used for Basic and Digest authentication only. For configuring credentials for a custom web application (e.g., form-based login), use the “HTTP login page” pull-down menu. Two checkboxes are available on this page: “Never send SMB credentials in clear text” and “Only use NTLMv2”. Both of these settings affect the security of credentials sent out during Nessus scans.

Using cleartext credentials in any fashion is not recommended! If the credentials are sent remotely, via a Nessus scan or e-mailing a policy to another administrator, the credentials could be intercepted by anyone with access to the network. Use encrypted authentication mechanisms whenever possible.

Malicious Process Detection (plugin 59275) allows you to upload a custom list of MD5 hashes to identify running processes on scanned hosts when plugin 65548 is enabled. The format of the file is one MD5 hash per line without any surrounding whitespace. Optionally, a description may be added by putting a comma after the hash and the text of the description to be displayed in the scan results. Lines beginning with a # symbol are treated as comments and are ignored. All other items are considered invalid.

```
# hashes for the foobar malware
11b95ccc1427be5f6c7f0e547bde34e6,foobar malware 1.0
333459378f2d53d861ed2819b8b298af,foobar malware 1.1
f80a405f55c2cd651e58a8fc59550830,foobar malware 1.2

# example.exe
4f8793a9c7560af2cb48f062cd7879af
```

The **Modbus/TCP Coil Access** (plugin 23817) drop-down menu item is dynamically generated by the SCADA plugins available with the ProfessionalFeed. Modbus uses a function code of 1 to read “coils” in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a “write coil” message. The defaults for this are “0” for the “Start reg” and “16” for the “End reg”.

Nessus SYN scanner (plugin 11219) and **Nessus TCP scanner** (plugin 10335) options allow you to better tune the native SYN and TCP scanner to detect the presence of a firewall.

Table 28 – Nessus SYN and TCP Scanner Settings

Value	Description
Automatic (normal)	This option can help identify if a firewall is located between the scanner and the target (**default**).
Disabled (softer)	Disables the **Firewall detection** feature.
Do not detect RST rate limitation (soft)	Disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.
Ignore closed ports (aggressive)	Will attempt to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.

News Server (NNTP) Information Disclosure (plugin 11033) can be used to determine if there are news servers that are able to relay spam. Nessus will attempt to post a news message to a NNTP (Network News Transport Protocol) server(s), and can test if it is possible to post a message to upstream news servers as well.

Table 29 – News Server (NNTP) Information Disclosure Settings

Option	Description
From address	The address that Nessus will use as it attempts to post a message to the news server(s). This message will delete itself automatically after a short period of time.
Test group name regex	The name of the news group(s) that will receive a test message from the specified address. The name can be specified as a regular expression (regex) so that the message can be posted to multiple news groups simultaneously. For example, the default value "**f[a-z]\.tests?**" will broadcast a mail message to all news groups with names that begin with any letter (from "a" to "z") and end with ".tests" (or some variation that matched the string). The question mark acts as an optional wildcard.
Max crosspost	The maximum number of news servers that will receive the test posting, regardless of the number of name matches. For example, if the Max crosspost is "**7**", the test message will only be sent to seven news servers, even if there are 2000 news servers that match the regex in this field.
Local distribution	If this option is selected, Nessus will only attempt to post a message to the local news server(s). Otherwise, an attempt will be made to forward the message upstream.

No archive	If this option is selected, Nessus will request to not archive the test message being sent to the news server(s). Otherwise, the message will be archived like any other posting.

Oracle settings (plugin 22076) allows the user to enter the Oracle database SID to specify which database to test. In addition, “Test default accounts (slow)” enables the Nessus scan to probe for default accounts within the remote database for vulnerabilities.

Palo Alto Networks PAN-OS Settings (plugin 64286) allows you to set the Username and Password for logging into a Palo Alto device. Additionally the Port may be customized and the ability to verify the SSL certificate presented.

Patch Management: IBM Tivoli Endpoint Manager Server Settings (plugin 62558) allows the user to enter credentials for an IBM Tivoli Endpoint Manager Server. If local credentials are not supplied for a system that is being scanned, the Tivoli Endpoint Manager server will be queried for and report the current patch status for the scanned host.

Patch Management: Red Hat Satellite Server Settings (plugin 57063) allows users to enter credentials for Red Hat Satellite servers. When a Red Hat host is scanned without local credentials, the Satellite server will be queried for and report the current patch status for the scanned host.

Patch Management: SCCM Server Settings (plugin 57029) allows users to enter credentials for a SCCM server. When a machine is scanned without local credentials, the SCCM server will be queried for and report the current patch status for the scanned host.

Patch Management: VMware Go Server Settings (plugin 57026) allows users to enter credentials for a VMware Go Server. When a machine is scanned without local credentials, the VMware Go server will be queried for and report the current patch status for the scanned host.

Patch Management: WSUS Server Settings (plugin 57031) allows users to enter credentials for a WSUS server. When a machine is scanned without local credentials, the WSUS server will be queried for and report the current patch status for the scanned host.

Ping the remote host (plugin 10180) options allow for granular control over Nessus’ ability to ping hosts during discovery scanning. This can be done via ARP ping, TCP ping, ICMP ping or applicative UDP ping.

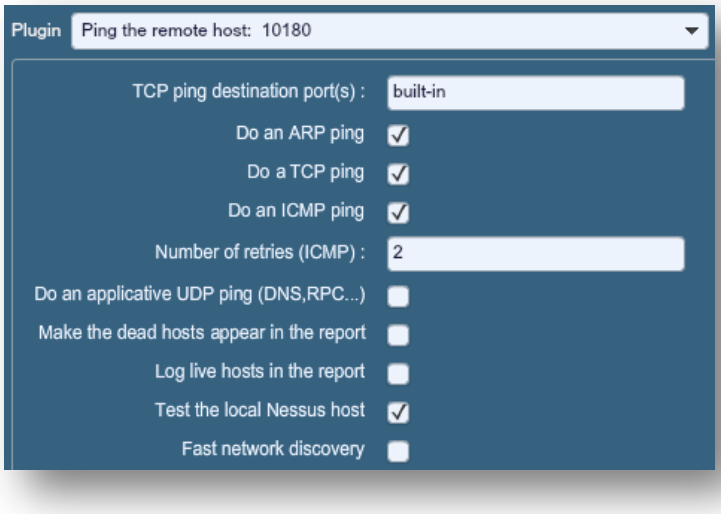

Plugin
Ping the remote host: 10180
TCP ping destination port(s) :
built-in
Do an ARP ping
Do a TCP ping
Do an ICMP ping
Number of retries (ICMP) :
2
Do an applicative UDP ping (DNS,RPC...)
Make the dead hosts appear in the report
Log live hosts in the report
Test the local Nessus host
Fast network discovery

Table 30 – Ping the Remote Host Settings

Option	Description
TCP ping destination port(s)	Specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting to the default of “built-in”.
Do an ARP ping	Utilize the ARP protocol for pings.
Do a TCP ping	Utilize the TCP protocol for pings.
Do an ICMP ping	Utilize the ICMP protocol for pings.
Number of Retries (ICMP)	Allows you to specify the number of attempts to try to ping the remote host. The default is set to 2.
Do an applicative UDP ping (DNS, RPC…)	Perform a UDP ping against specific UDP-based applications including DNS (port 53), RPC (port 111), NTP (port 123), and RIP (port 520).
Make the dead hosts appear in the report	If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts.
Log live hosts in the report	Select this option to specifically report on the ability to successfully ping a remote host.
Test the local Nessus host	This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.
Fast network discovery	By default, when Nessus “pings” a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1-65535 but there is no service behind). Such checks can take some time, especially if the remote host is firewalled. If the “fast network discovery” option is enabled, Nessus will not perform these checks.

Port scanner settings (plugin 33812) provide two options for further controlling port scanning activity:

Table 31 – Port Scanner Settings

Option	Description
Check open TCP ports found by local port enumerators	If a local port enumerator (e.g., WMI or `netstat`) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).
Only run network port scanners if local port enumeration failed	Rely on local port enumeration.

SMB Registry: Start the Registry Service during the scan (plugin 35703) enables the service to facilitate some of the scanning requirements for machines that may not have the “Remote Registry” service running all the time. The administrative shares may be enabled during the scan if they are not enabled at the beginning of the scan.

Under the **SMB Scope** (plugin 10917) menu, if the option “**Request information about the domain**” is set, then domain users will be queried instead of local users.

SMB Use Domain SID to Enumerate Users (plugin 10399) specifies the SID range to use to perform a reverse lookup on usernames on the domain. The default setting (1000 to 1200) is recommended for most scans.

SMB Use Host SID to Enumerate Local Users (plugin 10860) specifies the SID range to use to perform a reverse lookup on local usernames. The default setting (1000 to 1200) is recommended for most scans.

SMTP settings (plugin 11038) specify options for SMTP (Simple Mail Transport Protocol) tests that run on all devices within the scanned domain that are running SMTP services. Nessus will attempt to relay messages through the device to the specified "**Third party domain**". If the message sent to the "**Third party domain**" is rejected by the address specified in the "**To address**" field, the spam attempt failed. If the message is accepted, then the SMTP server was successfully used to relay spam.

Table 32 – SMTP Settings

Option	Description
Third party domain	Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.
To address	Nessus will attempt to send messages addressed to the mail recipient listed in this field. The **postmaster** address is the default value since it is a valid address on most mail servers.

SNMP settings (plugin 19762) allows you to configure Nessus to connect and authenticate to the SNMP service of the target. During the course of scanning, Nessus will make some attempts to guess the community string and use it for subsequent tests. If Nessus is unable to guess the community string and/or password, it may not perform a full audit against the service.

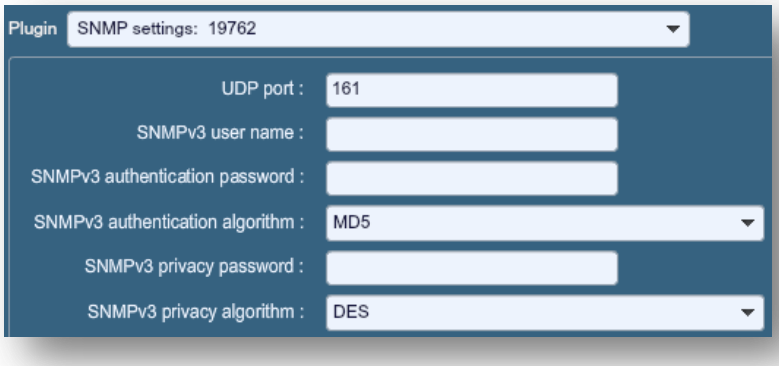


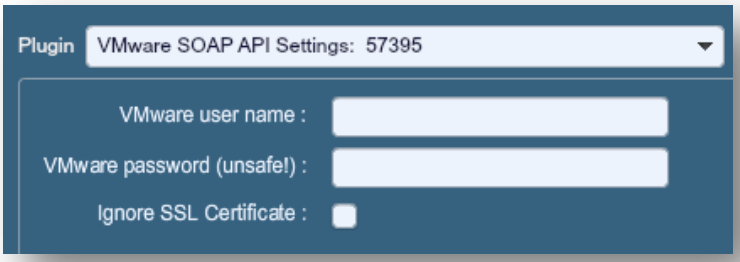
Table 33 – SNMP Settings

Option	Description
UDP port	Direct Nessus to scan a different port in the event that SNMP is running on a port other than 161.
SNMPv3 user name	The username for a SNMPv3 based account.
SNMPv3 authentication password	The password for the username specified.
SNMPv3 authentication algorithm	Select MD5 or SHA1 based on which algorithm the remote service supports.
SNMPv3 privacy password	A password used to protect encrypted SNMP communication.
SNMPv3 privacy algorithm	The encryption algorithm to use for SNMP traffic.

SSH settings (plugin 14273) – Users can select "**SSH settings**" from the drop-down menu and enter a "**`known_hosts`**" file for scanning Unix systems. There is also a field for entering the "Preferred SSH Port". By default Nessus will use the standard TCP port 22 for credentialed Unix scans; however, this setting enables the user to specify a non-standard port for SSH login attempts.

Service Detection (plugin 22964) controls how Nessus will test SSL based services: known SSL ports (e.g., 443), all ports, or none. Testing for SSL capability on all ports may be disruptive for the tested host.

VMware SOAP API Settings (plugin 57395) provides Nessus with the credentials required to authenticate to VMware ESX, ESXi, and vSphere Hypervisor management systems via their own SOAP API, as SSH access has been deprecated. This API is intended for auditing vSphere 4.x / 5.x, ESXi, and ESX hosts, not the virtual machines running on the hosts. This authentication method can be used to perform credentialed scans or perform compliance audits.



VMware vCenter SOAP API Settings (plugin 63060) provides Nessus with the credentials required to authenticate to VMware vCenter management systems via their own SOAP API. The API is intended to audit vCenter, not the virtual machines running on the hosts. This authentication method can be used to perform credentialed scans or perform compliance audits.

Wake-on-LAN (plugin 52616) controls what hosts to send WOL magic packets to before performing a scan and how long to wait (in minutes) for the systems to boot. The list of MAC addresses for WOL is entered using an uploaded text file with one host MAC address per line.

For example:

```
00:11:22:33:44:55
aa:bb:cc:dd:ee:ff
…
```

Web Application Tests Settings (plugin 39471) tests the arguments of the remote CGIs (Common Gateway Interface) discovered in the web mirroring process by attempting to pass common CGI programming errors such as cross-site scripting, remote file inclusion, command execution, traversal attacks, and SQL injection. Enable this option by selecting the “Enable web applications tests” checkbox. These tests are dependent on the following NASL plugins:

- 11139, 42424, 42479, 42426, 42427, 43160 – SQL Injection (CGI abuses)
- 39465, 44967 – Command Execution (CGI abuses)
- 39466, 47831, 42425, 46193, 49067 – Cross-Site Scripting (CGI abuses: XSS)
- 39467, 46195, 46194 – Directory Traversal (CGI abuses)
- 39468 – HTTP Header Injection (CGI abuses: XSS)
- 39469, 42056, 42872 –File Inclusion (CGI abuses)
- 42055 – Format String (CGI abuses)
- 42423, 42054 – Server Side Includes (CGI abuses)
- 44136 – Cookie Manipulation (CGI abuses)
- 46196 – XML Injection (CGI abuses)
- 40406, 48926, 48927 – Error Messages
- 47830, 47832, 47834, 44134 – Additional attacks (CGI abuses)

Note: This list of web application related plugins is updated frequently and may not be complete. Additional plugins may be dependent on the settings in this preference option.

The screen capture below is the “Web Application Tests Settings” input page:

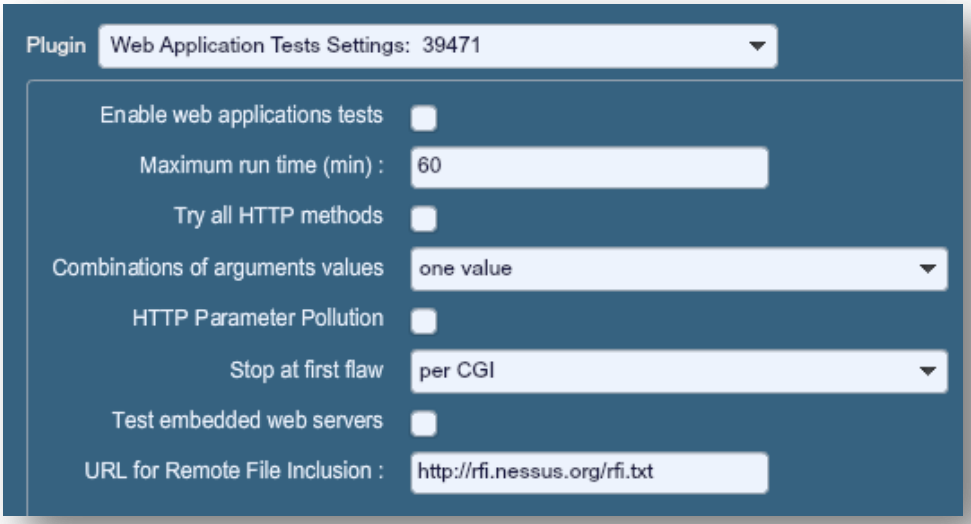


Table 34 – Web Application Tests Settings

Option	Description
Enable web applications tests	This check box enables web application tests and causes the settings below to be evaluated during the test.
Maximum run time (min)	This option manages the amount of time in minutes spent per NASL script performing web application tests. These NASL scripts are listed above. At the time of this writing, there were 36 web application test NASLs. The run time of each script varies widely, however the following generic formula applies to the Maximum_run_time: scan_time = (num_scripts/max_checks)*Maximum_run_time For example: (36/5) * 60 = 432 minutes This option defaults to 60 minutes and applies to all ports and CGIs for a given web site.
Try all HTTP methods	By default, Nessus will only test using GET requests. This option will instruct Nessus to also use “POST requests” for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required. When selected, Nessus will test each script/variable with both GET and POST requests.
Combinations of arguments values	This option manages the combination of argument values used in the HTTP requests. This drop-down has five options: **one value** – This tests one parameter at a time with an attack string, without trying

	"non-attack" variations for additional parameters. For example, Nessus would attempt "`/test.php?arg1=XSS&b=1&c=1`" where "b" and "c" allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. **some pairs** – Like "all pairs" testing, this will try to test a representative data set based on the "All-pairs" method. However, for each parameter discovered, Nessus will only test using a maximum of three valid input variables. **all pairs (slower but efficient)** – This form of testing is slightly slower but more efficient than the "one value" test. While testing multiple parameters, it will test an attack string, variations for a single variable, and then use the first value for all other variables. For example, Nessus would attempt "`/test.php?a=XSS&b=1&c=1&d=1`" and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for "`/test.php?a=XSS&b=3&c=3&d=3`" when the first value of each variable is "1". **some combinations** – Like "all combinations" testing, this will perform tests using a combination of attack strings and valid input. However, for each parameter discovered, Nessus will only test using a maximum of three valid input variables. **all combinations (extremely slow)** – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where "All-pairs" testing seeks to create a smaller data set as a tradeoff for speed, "all combinations" makes no compromise on time and uses a complete data set of tests. This testing method may take a **long** time to complete.
HTTP Parameter Pollution	When performing web application tests, attempt to bypass any filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like "`/target.cgi?a='&b=2`". With HTTP Parameter Pollution (HPP) enabled, the request may look like "`/target.cgi?a='&a=1&b=2`".
Stop at first flaw	This option determines when a new flaw is targeted. The drop-down has four options: **per CGI** (default) – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. **per port (quicker)** – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port. **per parameter (slow)** – As soon as one flaw is found in a parameter of a CGI, Nessus stops and switches to the next parameter of the same script. **look for all flaws (slower)** – Perform extensive tests regardless of flaws found. This option can take a long time and is not recommend in most cases.
Test embedded web servers	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.

URL for Remote File Inclusion	During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted on Tenable's web server for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.

Web mirroring (plugin 10662) sets configuration parameters for Nessus' native web server content mirroring utility. Nessus will mirror web content to better analyze the contents for vulnerabilities and help minimize the impact on the server.

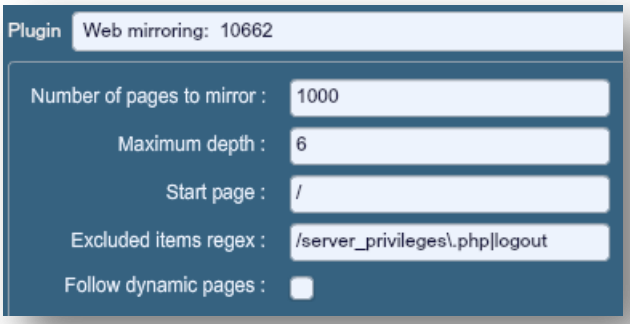


Table 35 – Web Mirroring Settings

Option	Description
Number of pages to mirror	The maximum number of pages to mirror.
Maximum depth	Limit the number of links Nessus will follow for each start page.
Start page	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., "/:/php4:/base").
Excluded items regex	Enable exclusion of portions of the web site from being crawled. For example, to exclude the "`/manual`" directory and all Perl CGI, set this field to: `(^/manual)|(\.pl(\?.*)?$).`
Follow dynamic pages	If this checkbox is selected, Nessus will follow dynamic links and may exceed the other "Web mirroring" parameters.

When all of the options have been configured as desired, click "**Submit**" to save the policy and return to the **Policies** tab. At any time, you can click "**Edit**" to make changes to a policy you have already created or click "**Delete**" to remove a policy completely.

Users

SecurityCenter administrators and predefined roles are configured via the "Users" tab. More than one administrator can be created per SecurityCenter. It is recommended to make at least one administrator user using TNS authentication. This will enable at least one administrator-level account to log in should the LDAP service become unavailable.

Administrators

The administrative user can create other administrator users; however, they may only modify the “Basic” fields for the new user being created. “Access” and “Resources” tabs are displayed, but administrative users cannot edit them. All administrators have the same permission level and resources. The table below details fields from the “Basic” view:

Table 36 – Basic Options for Adding Administrators

Option	Description
Authentication Information	
Type – TNS	
Username	This is the account name the user will use to log into SecurityCenter. When selecting this account name, it is sometimes easier to focus on the person’s real name as a convention (e.g., John Galt would become “jgalt”). However, it may also be useful to assign names based on role, such as “auditNY”. The username value is case-sensitive.
Password	The login password It is recommended to use passwords that meet stringent length and complexity requirements.
Type – LDAP	
Search String	This is the LDAP search string to use to narrow down user searches. Proper format is: “attribute=<filter text>”. Wildcards are permitted and the field accepts up to 1024 characters. For example: sAMAccountName=* mail=a* displayName=C*
Users	This box contains a list of users obtained from the configured LDAP server that match the Search String above.
Username	User that is selected from the list of users above.
Notification	
Email user their account information	When the user is created, you can choose to have them notified via email of their account by selecting this check box. If the following error message is received when attempting to add a user:

	`Error creating email notifying user 'test'. Invalid address: noreply@localhost` Check the **System** -> **Configuration** -> **Mail** -> **Return Address** settings. The email address defaults to “noreply@localhost” if left blank. Many email servers will disallow emails from this address.
Email user their password	There is an option to include the user’s password within the email if desired. If this is not included, contact information of the security manager will be included. (TNS Authentication only)
User must change their password on login	Require password change on next login. (TNS Authentication only)
Basic/Contact Information	
Name, Title, Address Information, Email, Phone	Contact information for the user can be entered here.

Roles

The pre-defined roles of Administrator, No Role, and Organization Head cannot be edited.

Roles determine what a user can or cannot do from their account. They can be configured to a great degree. SecurityCenter comes with five pre-defined roles; however, custom roles can be created by the Organization Head user to facilitate organizations with a complex security policy needs. In keeping with the SecurityCenter convention, role assignments are hierarchical. Users may only assign permissions that they currently own. For example, if a user has a custom role with “View Vulnerability Data” enabled and “Update Plugins” disabled, that user can only create users with “View Vulnerability Data” enabled.

Available pre-defined roles include:

- Administrator
- End User
- Manager
- No Role
- Organization Head

The Administrator, No Role, and Organization Head roles are static and cannot be modified. An administrator is an account that has management responsibility over the console. The primary task of the administrator is to install and configure each Organization. In addition, the administrator adds components to SecurityCenter such as PVS, LCE, and Nessus to extend its capabilities. The administrator is automatically assigned the “Manage Application” role.

An Organization Head is the account within an Organization that has a broad range of security roles within the defined Organization. This is the initial user that is created when a new Organization is created and has the ability to launch scans, configure users (except for the administrator user), vulnerability policies, and other objects that belong to their Organization. Each Organization has an **Organization Head** account that cannot be deleted. Permission-wise, the Organization Head user is nearly identical to the Manager user, however there are differences:

1. The Organization Head can add/edit/delete roles, while the Manager cannot.
2. The Organization Head can add users that are the subordinate of any Manager or User with the “Manage Users” permission. The Manager can only add users as a subordinate of themselves.
3. The Organization Head has visibility of scan schedules and report definitions for the entire Organization, while Managers can only see those of their subordinates.

Additional users may be created and assigned either one of three possible roles or a custom one. These roles are “Manager”, “End User”, and “No Role”.

The “Manager” role is intended for security team managers who have the need to manage end-user objects along with vulnerability, resource and scans. The Manager user is very similar in capability to the Organization Head user except that they cannot manage roles and cannot manage objects not in their hierarchy (all Organizational users are in the Organization Head’s hierarchy).

An end-user is an authorized system administrator, network engineer, or auditor with the ability to review their security data, create and view reports, enter in remediation actions to close tickets, and launch scans (if given proper credentials).

“No Role” is the default “catch-all” role for users or objects for which no role has been assigned or explicit roles have been removed. This role has virtually no permissions to perform actions within SecurityCenter.

User Access Control

Within the defined user roles, granular permissions are applied that enable users to perform various tasks. Custom roles can also be created with any combination of desired permissions based on enterprise needs.

Role permissions are broken down based on user visibility. In all cases except policy roles, an “Organizational” designation indicates that the user with that role can create objects with either “User” or “Organizational” visibility. In the case of scan policy creation, users with the “Create Policies” permission can only create policies with “User” visibility. Users with “Create Organizational Policies” and “Create Policies” permissions can create policies with either “User” or “Organizational” visibility. Users with only the “Create Organizational Policies” permission cannot create any scan policies.

The table below defines the various permissions available within the SecurityCenter architecture:

Table 37 – Available Permissions

Permission	Description	Organization Head	Administrator	Manager	End User
Accept Risks	Accept the risk of vulnerabilities	X		X	
Create Alerts	Create custom alerts	X		X	X
Create Audit Files	Upload custom audit files	X	X	X	X
Create Application Roles	Create roles with application visibility. This is not a configurable role.		X		
Create Organization Roles	Create roles with Organizational visibility. This is not a configurable role.	X			

Create Organization Assets	Create assets	X		X	X
Create Organization Credentials	Create credentials	X		X	X
Create Organization Policies	Create scan policies with Organizational visibility. This option must be used in conjunction with the “Create Policies” permission.	X		X	X
Create Organization Queries	Create queries	X		X	X
Create Policies	Create scan policies with “User” visibility. This option must be set for the “Create Organizational Policies” option to function. Use this option for users who will create policies for themselves, but, not shared policies. This can be useful for new users.	X		X	X
Create Tickets	Create tickets	X		X	X
Edit/Delete Organization Assets	Edit or delete assets belonging to the user’s Organization regardless of what Organizational user created it.	X			
Edit/Delete Organization Credentials	Edit or delete credentials belonging to the user’s Organization regardless of what Organizational user created it.	X			
Edit/Delete Organization Policy	Edit or delete policies belonging to the user’s Organization regardless of what Organizational user created it.	X			
Edit/Delete Organization Query	Edit or delete queries belonging to the user’s Organization regardless of what Organizational user created it.	X			
Manage Applications	Manage SecurityCenter applications and services. Any role with the “Manage Applications” permission is non-editable. The permission column is removed.		X		
Manage Users	Manage non-administrative users.	X		X	
Purge Tickets	Purge tickets	X		X	
Recast Risk	Recast the risk of vulnerabilities.	X		X	
Scan Privileges	Perform Nessus scans.	X		X	X
Share Assets	Share assets with other users.	X		X	X

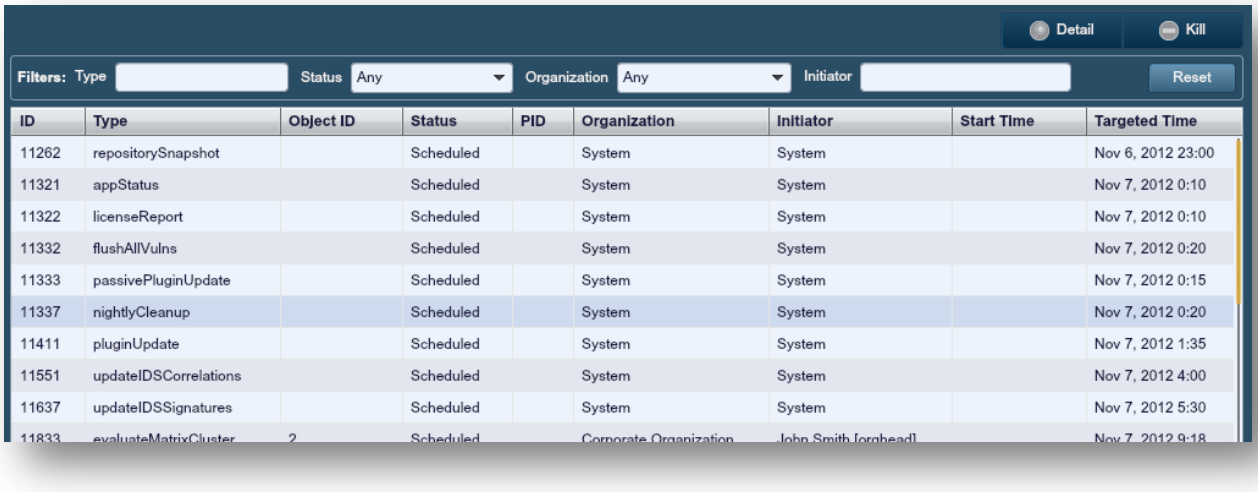
Share Credentials	Share credentials with other users.	X		X	X
Share Dashboard Tabs	Share dashboard tabs with other users.	X		X	X
Share Policies	Share policies with other users.	X		X	X
Share Queries	Share queries with other users.	X		X	X
Update Plugins	Update Active, Passive, and Custom plugins.	X		X	X
Upload Nessus Scan Results	Upload Nessus scan results.	X		X	X
View Event Data	View event data.	X		X	X
View Organization Logs	View Organization logs.	X		X	
View Vulnerability Data	View vulnerabilities within the Organizational repository.	X		X	X
Manage Attribute Sets	Create and manage CyberScope and ARF attribute sets for reports	X		X	

Note that as listed above, the Manager and User roles reflect the default settings. These two roles are editable.

Status

Job Queue

The SecurityCenter Job Queue contains a listing of scheduled and running jobs along with job metadata.


Detail
Kill
Filters: Type
Status
Any
Organization
Any
Initiator
Reset
ID
Type
Object ID
Status
PID
Organization
Initiator
Start Time
Targeted Time
11262 repositorySnapshot Scheduled System System Nov 6, 2012 23:00
11321 appStatus Scheduled System System Nov 7, 2012 0:10
11322 licenseReport Scheduled System System Nov 7, 2012 0:10
11332 flushAllVulns Scheduled System System Nov 7, 2012 0:20
11333 passivePluginUpdate Scheduled System System Nov 7, 2012 0:15
11337 nightlyCleanup Scheduled System System Nov 7, 2012 0:20
11411 pluginUpdate Scheduled System System Nov 7, 2012 1:35
11551 updateIDSCorrelations Scheduled System System Nov 7, 2012 4:00
11637 updateIDSSignatures Scheduled System System Nov 7, 2012 5:30
11833 evaluateMatrixCluster 2 Scheduled Corporate Organization John Smith [orghead] Nov 7, 2012 9:18

Available fields include Job ID, Type, Obj ID, Status, PID, Organization, Initiator, Start Time, and Targeted Time. This information is not generally required for the day to day operations of SecurityCenter, but may be requested by Tenable Support when troubleshooting issues.

Job options include "**Detail**", which lets you view individual job details and "**Kill Job**", which lets you kill a currently running job. Killing any process is not recommended except at the request of Tenable Support.

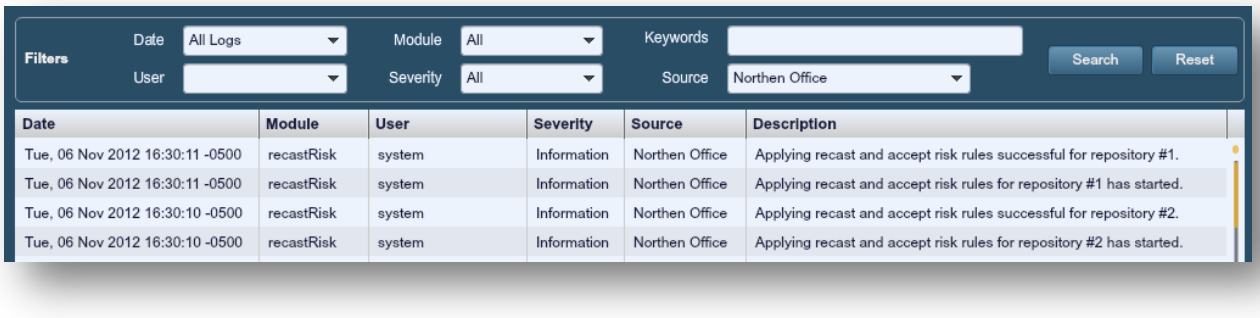
Jobs may be searched using the "Filters" bar at the top of the page. The available filters are "Type", "Status", "Organization", and "Initiator". These filters may be used individually or in combination to narrow the displayed list of jobs.

Table 38 – Filters

Option	Description
Type	This is a text field that will narrow the search as you type. It will match on the text entered and is not case sensitive.
Status	This will display the jobs with the selected status.
Organization	Only the jobs owned by the selected organization will be displayed.
Initiator	Only the jobs owned by the initiator with the name or partial name entered in the field will be displayed.

Logs

SecurityCenter logs contain detailed filter options to troubleshoot unusual system or user activity. The logs include filters that allow users to search logs based on parameters such as date, user, module, severity, keywords, and source. An example keyword and source search based on the word "attempt" is displayed below:



This search flexibility improves debugging and maintains an audit trail of users who access SecurityCenter or perform basic functions such as changing passwords, recasting risks, or running Nessus scans.

Audit Admin & User Activity

SecurityCenter provides the ability to audit user activity either through the console web interface or via a flat ASCII log file in the `/opt/sc4/orgs/[organization id]/logs` and `/opt/sc4/admin/logs` directories on the SecurityCenter server. Authorized system administrators are also able to sort through audit data using operating system commands such as "grep", "awk", and "sed".

Startup and Shutdown of the Audit Functions

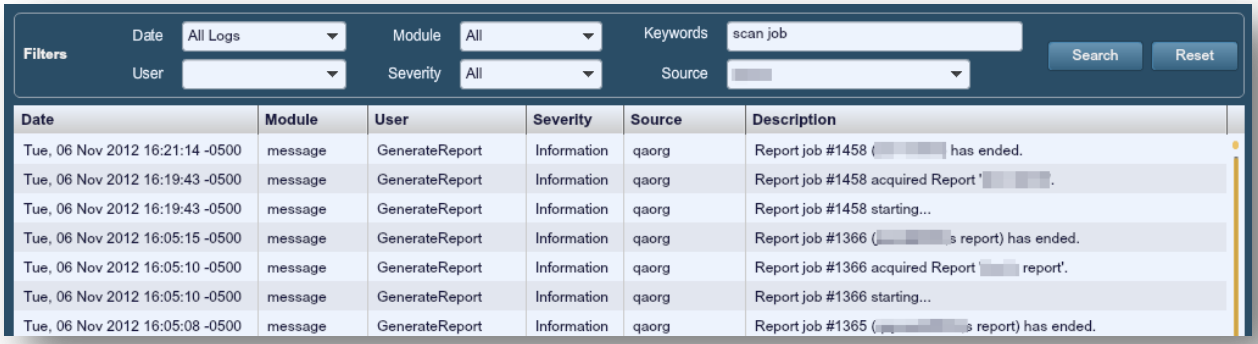
The audit functions are built into the SecurityCenter application and are started when SecurityCenter is started, usually at system boot time or manually by a system administrator. The audit functions cannot be shut down while SecurityCenter is running.

Accessing the Audit Records

To access the user activity data via the web interface, you must be logged into the Security Center console as the **admin** user and, from the "Status" tab, select the "Logs" option.

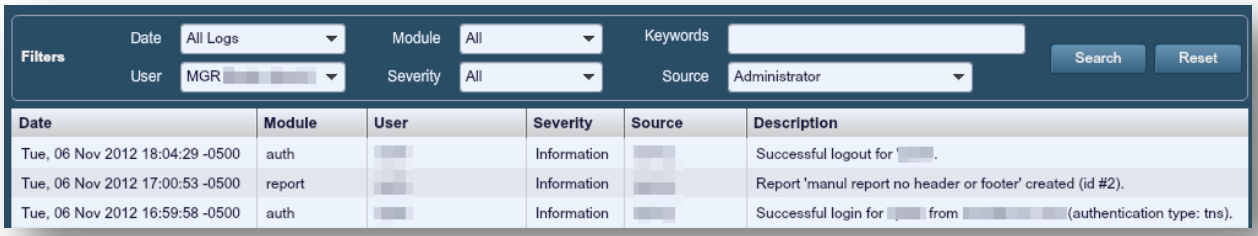
Login records are written every time a SecurityCenter user attempts to access SecurityCenter. The following screen capture shows some examples of this activity:

In addition to login activity, information regarding successful and unsuccessful attempts to launch scans is displayed.



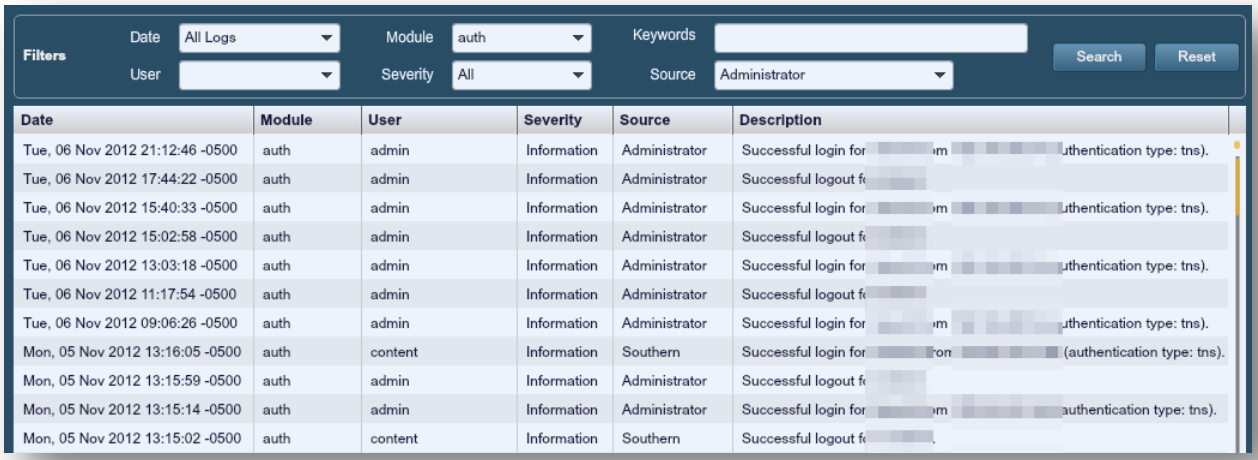
The web interface to search these logs defaults to "All Logs". Log files can be selected by month if present. Logs may be searched by typing in keywords or combinations of keywords, although regular expressions and wild cards are not supported.

For example, to monitor the activities of one particular user, simply select the username in the drop-down box as shown in the following screen:

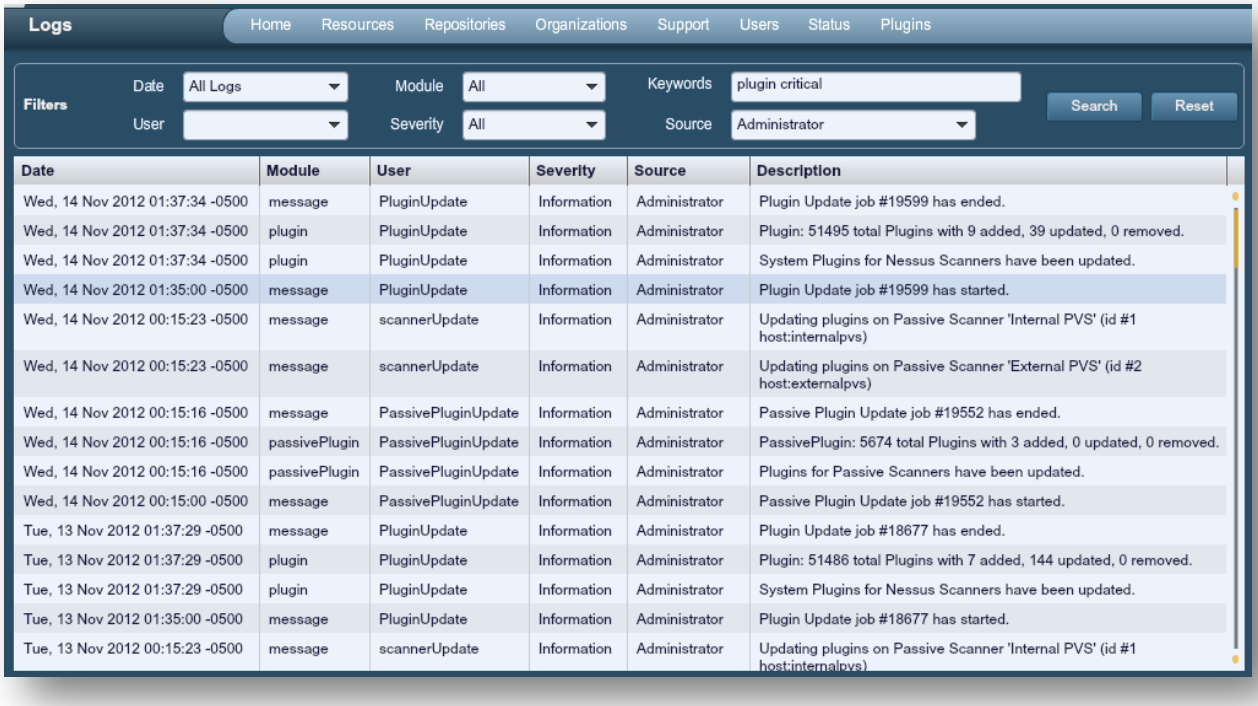


Logs can be searched and filtered by type of SecurityCenter event, event success or event failure by using relevant filters and keywords for each particular type of search. Event failures are listed as “Critical” or “Warning” for each type of event, as shown in the examples below for SecurityCenter authentication attempts:

In contrast, successful events can be searched and filtered by selecting a particular module for event type and filtering by the keyword “success”:



Logs can also be searched and viewed to show errors received from Nessus, the LCE, and the PVS. In the example below, a keyword of “plugin” was used in conjunction with a severity of “Critical” to list errors related to the updates of PVS plugins:



Date	Module	User	Severity	Source	Description
Wed, 14 Nov 2012 01:37:34 -0500	message	PluginUpdate	Information	Administrator	Plugin Update job #19599 has ended.
Wed, 14 Nov 2012 01:37:34 -0500	plugin	PluginUpdate	Information	Administrator	Plugin: 51495 total Plugins with 9 added, 39 updated, 0 removed.
Wed, 14 Nov 2012 01:37:34 -0500	plugin	PluginUpdate	Information	Administrator	System Plugins for Nessus Scanners have been updated.
Wed, 14 Nov 2012 01:35:00 -0500	message	PluginUpdate	Information	Administrator	Plugin Update job #19599 has started.
Wed, 14 Nov 2012 00:15:23 -0500	message	scannerUpdate	Information	Administrator	Updating plugins on Passive Scanner 'Internal PVS' (id #1 host:internalpvs)
Wed, 14 Nov 2012 00:15:23 -0500	message	scannerUpdate	Information	Administrator	Updating plugins on Passive Scanner 'External PVS' (id #2 host:externalpvs)
Wed, 14 Nov 2012 00:15:16 -0500	message	PassivePluginUpdate	Information	Administrator	Passive Plugin Update job #19552 has ended.
Wed, 14 Nov 2012 00:15:16 -0500	passivePlugin	PassivePluginUpdate	Information	Administrator	PassivePlugin: 5674 total Plugins with 3 added, 0 updated, 0 removed.
Wed, 14 Nov 2012 00:15:16 -0500	passivePlugin	PassivePluginUpdate	Information	Administrator	Plugins for Passive Scanners have been updated.
Wed, 14 Nov 2012 00:15:00 -0500	message	PassivePluginUpdate	Information	Administrator	Passive Plugin Update job #19552 has started.
Tue, 13 Nov 2012 01:37:29 -0500	message	PluginUpdate	Information	Administrator	Plugin Update job #18677 has ended.
Tue, 13 Nov 2012 01:37:29 -0500	plugin	PluginUpdate	Information	Administrator	Plugin: 51486 total Plugins with 7 added, 144 updated, 0 removed.
Tue, 13 Nov 2012 01:37:29 -0500	plugin	PluginUpdate	Information	Administrator	System Plugins for Nessus Scanners have been updated.
Tue, 13 Nov 2012 01:35:00 -0500	message	PluginUpdate	Information	Administrator	Plugin Update job #18677 has started.
Tue, 13 Nov 2012 00:15:23 -0500	message	scannerUpdate	Information	Administrator	Updating plugins on Passive Scanner 'Internal PVS' (id #1 host:internalpvs)

The flat ASCII log file used to store the customer activity data is rolled over every month and may be archived in accordance with local site backup procedures. For example, a log file for the month of November 2012 would be named `/opt/sc4/orgs/1/logs/201211.log`. When the month changes to December, this log file will be preserved and a new log file will be created and named `/opt/sc4/orgs/1/logs/201212.log`.

Modification to the Audit Configuration and Administrator Log

There is no configuration option to enable another user to view the Administrator logs or to turn off the audit function. The audit functionality is built into the application, is always on, and there are no options available to disable it except to shut down the application, which is logged by SecurityCenter. The only other possible way to disable the audit functions is to modify the source code, which is not available to end users. Through the SecurityCenter web interface, SecurityCenter audit trail log files are read-only and are not able to be modified or deleted. These log files are also protected from unauthorized access and/or deletion by file and group permissions that only allow the “root” and “tns” users (e.g., authorized system administrators) to access the files through the SecurityCenter server via console, and system accesses are logged through standard functions (e.g., `/var/log/messages`, `/var/log/secure`, etc.) by the underlying host operating system.

Audit Log Data Selection

In conjunction with the LCE, SecurityCenter can be configured to provide more granular options for the selection of audit log data. Refer to Appendix 7, “Configuring SecurityCenter and the LCE for Audit Data Selection” for details on additional configuration options.

Plugins

Plugins are scripts used by the Nessus, PVS, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and PVS plugins are managed centrally by SecurityCenter and pushed out to their respective scanners. LCE servers download their own event plugins and SecurityCenter downloads event plugins for its local reference. SecurityCenter does not currently push event plugins to LCE servers.

Within the **Plugins** interface, the user has the ability to perform a wide variety of plugin-related functions including updating active, passive and event plugins, upload custom plugins, view plugin details/source, and search for specific plugins. Clicking on the "**Plugins**" tab displays a page similar to the one below:

Update Plugins

Immediately after installing SecurityCenter, plugins are automatically updated on a regular basis. Manually updating plugins simply involves clicking on the "Update Plugins" button and waiting for the process to complete. Due to the large quantity of plugins and inconsistency of network speeds, this process can take a long time to complete. Please refer to Appendix 5 of this document for more information about performing offline plugin updates with SecurityCenter.

The date and time of the last successful plugin update is displayed for each type at the top of the page to the right of the "Upload Plugins" command button. After a successful download, the plugins are displayed in the plugin table with the date or number of hours or days of the last successful download in the "Date Downloaded" field.

Upload Plugins

Clicking on "**Upload Plugins**" opens a dialog box that allows the user to upload one or more active, passive, event, or custom plugins. Choose "**Custom**" for any active, passive or event plugins that you have created. All custom plugins must have unique Plugin ID numbers and have family associations based on existing SecurityCenter families. Choose "**Active**", "**Passive**", or "**Event**" for the appropriate type of Tenable provided signed plugins.

Custom plugin uploads must be a complete "feed". In order to upload custom plugins, the provided **`tar.gz`** file must include the relevant NASLs and a "**`custom_feed_info.inc`**" file comprised of the following two lines:

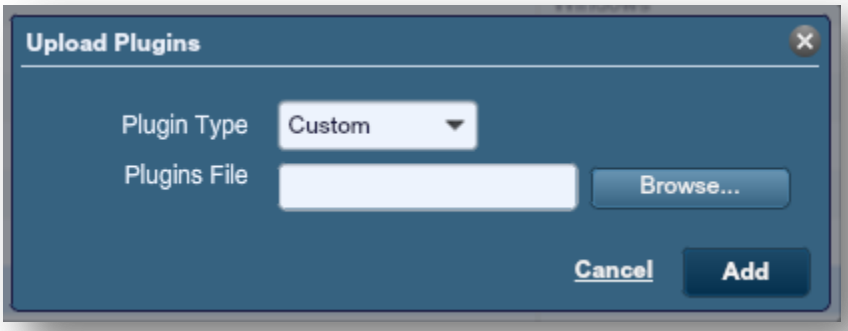
```
PLUGIN_SET = "201202131526";
PLUGIN_FEED = "Custom";
```

The administrator must manage this file and update the PLUGIN_SET option for each upload. The PLUGIN_SET format is "YYYYMMDDHHMM".

For example, running the following command against the "**`custom_feed_info.inc`**" file and custom plugins in a directory will create a new tar and gziped uploadable archive file called **`custom_nasl_archive.tar.gz`** that contains both custom plugins:

```
# tar -cvzf custom_nasl_archive.tar.gz custom_feed_info.inc *.nasl
```

It is recommended that the `custom_nasl_archive.tar.gz` file be updated for each addition and update of custom NASLs.



After browsing for the plugin archive and uploading it, confirm the plugin type and then click "**Add**" to extract the plugins to SecurityCenter. Shortly after completion a notification message is displayed indicating a successful plugin upload.

Other Plugin Options

Other plugin options include "**Detail**" and "**Source**". The "Detail" option loads a pop-up with plugin details such as Plugin ID, Plugin Name, Family, Plugin Type, Version, Plugin Publication Date, Plugin Modification Date, CVE/BID, CVSS Score, CVSS Vector, if an exploit is available, Description, and Solution. The "Source" option displays the plugin source code, as available, to the user. The "**Search**" option allows you to search for plugins based on several plugin attributes including: ID, Name, Description, Type, CVEBID (CVE or Bugtraq ID number), MSFT (Microsoft Bulletin), XRef, and Exploit Available.

Troubleshooting

SecurityCenter

SecurityCenter does not appear to be operational

- Close and reopen the web browser if a login page does not appear. Ensure that Adobe Flash is installed and able to run on the target system's web browser.
- Ensure that the remote **`httpd`** service is running on the SecurityCenter host:

  ```
  # ps ax | grep httpd

  1990 ?        Ss     0:01 /opt/sc4/support/bin/httpd -k start
  ```

- Ensure that sufficient drive space exists on the SecurityCenter host:

  ```
  # df

  Filesystem                1K-blocks       Used  Available   Use% Mounted on
  /dev/mapper/VolGroup00-LogVol00
                          8506784    8506784          0   100% /
  /dev/sda1                101086      24455      71412    26% /boot
  tmpfs                   1037732          0    1037732     0% /dev/shm
  ```

  If drive space has become exhausted for any reason, sufficient space must be recovered and the SecurityCenter service must be restarted for SecurityCenter to become operational:

  ```
  # df

  Filesystem         1K-blocks       Used  Available   Use% Mounted on
  /dev/mapper/VolGroup00-LogVol00
                           8506784    6816420    1251276    85% /
  ```

```
/dev/sda1                     101086      24455      71412    26% /boot
tmpfs                   1037732          0    1037732     0% /dev/shm

# service SecurityCenter restart

Shutting down SecurityCenter services:                     [  OK  ]
Starting SecurityCenter services:                          [  OK  ]
#
```

Forgot login credentials

- Contact Tenable Support (support@tenable.com).

Invalid license error

- If you receive an invalid license error while attempting to log in as an Organization Head or lower, an administrator must log in and upload a new valid license key. A user with access to the host OS and valid permissions can also check that an up-to-date license exists in **/opt/sc4/daemons**. Licenses are obtained from Tenable and copied to the daemons directory as the "tns" user.

```
-rw-r--r--  1 tns tns    1942 Oct 29 12:14 license.key
```

Reporting does not work

- Check your Java version. Only OpenJDK and Oracle JRE are supported. The existence of another type of Java on the system will break reporting.

LCE

LCE server does not appear to be operational:

- Log into the SecurityCenter UI as admin and confirm that the LCE server state is "Working" along with all attached LCE clients.
- Check that you can SSH from the SecurityCenter host to the LCE host.
- Check that the LCE daemon is running on its host and listening on the configured port (TCP port 31300 by default):

```
# netstat -pan | grep lced

tcp        0      0 0.0.0.0:31300   0.0.0.0:*     LISTEN      30339/lced
```

- Check that the listening ports can be reached from the network and are not blocked by a firewall.
- If the LCE server is not operational, attempt to start the service:

```
# service lce start

Starting Log Correlation EngineLCE Daemon Configuration
LICENSE: Tenable Log Correlation Engine 3-Silo Key for [user]
 EXPIRE: 11-10-011
 REMAIN: 30 days
MESSAGE: LCE (3-silo license)
MESSAGE: Valid authorization
-------------------------------------------------------
                                                           [  OK  ]
```

No events from an attached LCE server

- Log into the SecurityCenter UI as admin and confirm that the LCE server state is "Working" along with all attached LCE clients.
- Confirm connectivity by checking that heartbeat events show up in the SecurityCenter UI.

- Check the **lce.conf** configuration file at "**/opt/lce/daemons/lce.conf**" in accordance with the LCE documentation.
- Check the individual LCE client configuration and authorization in the LCE Clients screen. If syslog is being used to collect information and events, ensure that the syslog service is running and configured correctly on the target syslog server in accordance with LCE documentation.
- Check for NTP time synchronization between the SecurityCenter, LCE, and LCE clients.

Invalid LCE license

- Check that an up-to-date license exists in **/opt/lce/daemons**. Licenses are obtained from Tenable and copied to the daemons directory with the name "**lce.key**".

```
-rw-r--r--  1 root root    1779 Oct  4 14:43 lce.key
```

Nessus

Nessus server does not appear to be operational:

- Verify in the SecurityCenter UI that the Nessus scanner appears as "Unable to Connect" under "Status".
- SSH to the remote Nessus host to make sure the underlying operating system is operational.
- Confirm that the Nessus daemon is running (Linux example below):

```
# service nessusd status
nessusd (pid 3853) is running...
```

- If the Nessus service is not running, start the service:

```
# service nessusd start
Starting Nessus services:
# ps -ef | grep nessusd
root      8201  8200 60 11:41 pts/2    00:00:05 nessusd -q
root      8206  7842  0 11:41 pts/2    00:00:00 grep nessusd
#
```

Cannot add a Nessus server

- Make sure the Nessus daemon was registered using the SecurityCenter option for registration.
- Check connectivity by telnetting from the SecurityCenter to the Nessus system on port 8834. If successful, the response will include: **Escape character is '^]'.**

Nessus scans fail to complete

- Ensure that the Nessus service is running on the Nessus host.
- Ensure that Nessus scanner is listed in SecurityCenter under "Resources" and "Nessus Scanners" and that the status of the Nessus scanner is listed as "Working". Click "Edit" to ensure that the IP address or hostname, port, username, password, and selected repositories for the Nessus scanner are all correct. Edit any incorrect entries to their correct state and click "Submit" to attempt to reinitialize the Nessus scanning interface.
- Right click the scan results and click "Scan Details" to obtain a more detailed description of the error. If the scan details indicate a "Blocking" error, this is indicative of a license IP count that has reached the limit. Either remove a repository to free up IP addresses or obtain a license for more IP addresses.
- Ensure that scan targets are permitted within the configured scan zones.

Nessus plugins fail to update

- Under “System” and “Configuration” in SecurityCenter, ensure that the Nessus Activation Code is marked as “Valid”.
- Ensure that the user used to connect to the Nessus server is configured as an ‘admin’ class user.
- Ensure that the SecurityCenter system is allowed outbound HTTP(S) connectivity to the Nessus Plugin Update Site. If it is not, refer to the Nessus 5.0 Installation and Configuration Guide for information on offline plugin updates.
- Under “System”, “Configuration”, and “Update” in SecurityCenter, ensure that Active Plugins is not set to “Never”. Manually test a plugin update under “Plugins” with “Update Plugins”. If successful, the line “Active Plugins Last Updated” will update to the current date and time.
- For all other Nessus plugin update issues, contact Tenable Support at support@tenable.com.

PVS

PVS server does not appear to be operational

- Verify in the SecurityCenter GUI that the PVS server appears as “Unable to Connect” under “Status”.
- SSH to the remote PVS host to make sure the underlying operating system is operational.
- Confirm that the PVS daemon is running (Linux example below):

```
# service pvs status

PVS is stopped
PVS Proxy (pid 3142) is running
#
```

If the PVS service is not running, start the service:

```
# service pvs start
Starting PVS Proxy                                         [  OK  ]
Starting PVS                                               [  OK  ]
#
```

Can’t add a PVS server

- Confirm that the PVS proxy is listening on port 1243:

```
# netstat -pan | grep 1243
tcp        0      0 0.0.0.0:1243    0.0.0.0:*     LISTEN      406/pvs-proxy
```

- Check connectivity by telnetting from the SecurityCenter to the PVS server on port 1243 (the **pvs-proxy**). If successful, the response will include: **Escape character is '^]'.**

No vulnerabilities are being received from the PVS server

- Ensure that the PVS service is running on the PVS host.
- Ensure that the PVS is listed in SecurityCenter under “Resources” and “Passive Scanners” and that the status of the PVS is listed as “Working”. Click “Edit” to ensure that the IP address or hostname, port, username, password, and selected repositories for the PVS are all correct. Edit any incorrect entries to their correct state and click “Submit” to attempt to reinitialize the PVS’ scanning interface.

PVS plugins fail to update

- Manually test a plugin update under “Plugins” with “Update Plugins”. If successful, the line “Passive Plugins Last Updated” will update to the current date and time.

- Ensure that the SecurityCenter host is allowed outbound HTTP(S) connectivity to the PVS Plugin Update Site.
- For all other PVS plugin update issues, contact Tenable Support at support@tenable.com.

Appendix 1: Non-Tenable License Declarations

Below you will find third-party software packages that Tenable provides for use with SecurityCenter 4.

Section 1 (b) (ii) of the SecurityCenter License Agreement reads:

(ii) The Software may include code or other intellectual property provided to Tenable by third parties, including Plug-Ins that are not owned by Tenable, (collectively, "Third Party Components"). Any Third Party Component that is not marked as copyrighted by Tenable is subject to other license terms that are specified in the Documentation. By using the Software, you hereby agree to be bound by such other license terms as specified in the Documentation.

SecurityCenter's Software License Agreement can be found on the machine SecurityCenter is installed on in the directory **`/opt/sc4/admin/misc`**.

Related Third-Party and Open-Source Licenses

- Apache – http://www.apache.org/licenses/LICENSE-2.0
- CoSign – http://weblogin.org/license.shtml
- glibc – http://www.gnu.org/copyleft/lesser.html
- HTMLDOC – http://www.gnu.org/copyleft/gpl.html
- jQuery – http://jquery.org/license
- libcURL – http://curl.haxx.se/docs/copyright.html
- libpng – http://www.libpng.org/pub/png/src/libpng-LICENSE.txt
- libxml2 – http://www.opensource.org/licenses/mit-license.html
- Nessus Plugins (not copyrighted to Tenable) – http://www.gnu.org/copyleft/gpl.html
- OpenLDAP – http://www.openldap.org/software/release/license.html
- OpenSSL – http://www.openssl.org/source/license.html
- PHP – http://us3.php.net/license/3_01.txt
- PHPMailer – (http://phpmailer.worxware.com/index.php) – http://www.gnu.org/copyleft/lgpl.html
- SQLlite – http://www.sqlite.org
- YUI – http://developer.yahoo.com/yui/license.html

This product includes cryptographic software written by Eric Young (eay@mincom.oz.au).
Copyright (C) 1995-1997 Eric Young. All rights reserved.
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Tenable Third-Party Licensed Software

ChartDirector Version 5.0

ChartDirector Version 5.0.2
Copyright (C) 2009 Advanced Software Engineering Limited
All Rights Reserved

********** LICENSE AGREEMENT **********

You should carefully read the following terms and conditions before using the ChartDirector software. Your use of the ChartDirector software indicates your acceptance of this license agreement. Do not use the ChartDirector software if you do not agree with the license agreement.

Disclaimer of Warranty

The ChartDirector software and the accompanying files are distributed and licensed "as is". Advanced Software Engineering Limited disclaims all warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose. Should the ChartDirector software prove defective, the licensee assumes the risk of paying the entire cost of all necessary servicing, repair, or correction and any incidental or consequential damages. In no event will Advanced Software Engineering Limited be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information and the like) arising out of the use or the inability to use the ChartDirector software even if Advanced Software Engineering Limited has been advised of the possibility of such damages.

Intellectual Property

The ChartDirector software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The ChartDirector software is licensed, not sold. Title to the ChartDirector software shall at all times remain with Advanced Software Engineering Limited.

You agree not to modify, decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the ChartDirector software.

Trial Version

The trial version of the ChartDirector software will produce yellow banner messages at the bottom of the chart images generated by it. You agree to not remove, obscure, or alter this message.

Subjected to the conditions in this license agreement:

- You may use the unmodified trial version of the ChartDirector software without charge.

- You may redistribute the unmodified trial version of the ChartDirector software, provided you do not charge for it.

- You may embed the unmodified trial version of the ChartDirector software (or part of it), in a product and distribute the product, provided you do not charge for the product.

If you do not want the yellow banner messages appearing in the charts, or you want to embed the ChartDirector software (or part of it) in a product that is not free, you must purchase a commercial license to use the ChartDirector software from Advanced Software Engineering Limited. Please refer to Advanced Software Engineering's web site at www.advsofteng.com for details.

Credits

The ASP/COM/VB, PHP, Perl, Python, Ruby and C++ editions of ChartDirector contains code from the Independent JPEG Group and the FreeType team. Any software that is derived from these editions of ChartDirector must include the following text in its documentation. This applies to both the trial version as well as to the commercial licensed version of ChartDirector.

- This software is based in part on the work of the Independent JPEG Group

- This software is based in part of the work of the FreeType Team

Nessus Plugins

Nessus Plugins (copyrighted by Tenable) – http://cgi.tenable.com/Subscription_Agreement.pdf

Appendix 2: Manual LCE Key Exchange

A manual key exchange between SecurityCenter and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote LCE to recognize SecurityCenter, you need to copy the SSH public key of SecurityCenter and append it to the "**/opt/lce/.ssh/authorized_keys**" file. The "**/opt/lce/daemons/lce-install-key.sh**" script performs this function. The following steps describe how to complete this process:

The LCE server must have a valid license key installed and the LCE daemon must be running before performing the steps below.

1. Download the SSH public key for SecurityCenter by logging in as the SecurityCenter administrator user and navigating to the "Keys" section ("**System**" -> "**Keys**").

2. Click "Download Key", choose the desired key format (both DSA or RSA work for this process) and then click "Submit".

3. Save the key file (**SSHKey.pub**) to your local workstation. Do not edit the file or save it to any specific file type.

4. From the workstation where you downloaded the key file, use a secure copy program, such as "scp" or "WinSCP" to copy the SSHKey.pub file to the LCE system. You will need to have the credentials of an authorized user on the LCE server to perform this step. For example, if you have a user "bob" configured on the LCE server (hostname "lceserver") whose home directory is /home/bob, the command on a Unix system would be as follows:

   ```
   # scp SSHKey.pub bob@lceserver:/home/bob
   ```

5. On the LCE server, as the root user, change the ownership of the ssh key file to lce as follows:

   ```
   # chown lce /home/bob/lce
   ```

   Then append the SSH public key to the "**/opt/lce/.ssh/authorized_keys**" file with the following steps:

   ```
   # su lce
   # /opt/lce/daemons/lce-install-key.sh /home/bob/SSHKey.pub
   ```

6. To test the communication, as the user "tns" on the SecurityCenter system, attempt to run the id command:

   ```
   # su tns
   # ssh -C -o PreferredAuthentications=publickey lce@<LCE-IP> id
   ```

   If a connection has not been previously established, you will see a warning similar to the following:

   ```
   The authenticity of host '192.168.15.82 (192.168.15.82)' can't be established.
   RSA key fingerprint is 86:63:b6:c3:b4:3b:ba:96:5c:b6:d4:42:b5:45:37:7f.
   Are you sure you want to continue connecting (yes/no)?
   ```

   Answer "yes" to this prompt.

   If the key exchange worked correctly, a message similar to the following will be displayed:

   ```
   # uid=251(lce) gid=251(lce) groups=251(lce)
   ```

7. The IP address of SecurityCenter can be added to the LCE system's /etc/hosts file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.

8. The LCE can now be added to SecurityCenter via the normal administrator "LCE add" process documented in the SecurityCenter 4.2 Administration Guide.

Appendix 3: Nessus SSL Configuration

Introduction

This section describes how to generate and exchange SSL certificates for the Nessus vulnerability scanner to use with SecurityCenter. For this procedure, you will need to have administrative (root) access to the SecurityCenter system, as well as all Nessus scanner systems.

Please note that users should be familiar with PKI deployments and it is not recommended that the Nessus server be used as the site's PKI system. The method described here is intended to assist in testing the functionality of the certificate exchange to assist users in the incorporation of the certificates into their current PKI system. In this method, the same key is shared between multiple servers. This may not be acceptable in some installations.

Overview of SSL Certificates and Keys

Nessus supports authentication protocols based on the OpenSSL toolkit (please see http://www.openssl.org/ for more details about the toolkit). This provides cryptographic protection and secure authentication. This section provides an overview of the certificates and keys necessary for SSL communication with Nessus. In the example described in this document, there are three key system components: the Certificate Authority, the Nessus Server and the Nessus client, which in this case is SecurityCenter. It is necessary to generate the keys required for the SSL communication and copy them to the appropriate directories.

Certificate Authority

The Certificate Authority (CA) ensures that the certificate holder is authentic and not an impersonator. The Certificate Authority holds a copy of the certificates for registered users to certify that the certificate is genuine. When the Certificate Authority receives a Certificate Signing Request (CSR), it validates and signs the certificate. In the example provided in this document, the Certificate Authority resides on the Nessus server, but this is not the recommended method for a production environment. In proper PKI deployments, the Certificate Authority would be a separate system or entity, such as Thawte or Verisign.

Nessus Server

In the example described in this document, the Nessus server is the same physical system that holds the Certificate Authority, but this will not likely be the case in a production environment. The Nessus server is the target of the secure communication and its keys must be generated locally and copied to the systems that will need to communicate with it using the SSL protocol. The Nessus server has users defined that authenticate to it either by simple login and password or via SSL. These users will also have keys associated with them.

Nessus Client

The Nessus client, which is SecurityCenter in this case, communicates with the Nessus server via SSL. It uses keys generated for a Nessus client and stores these keys and the certificate for the Certificate Authority in the `/opt/sc4/daemons` directory. These keys must be owned by the "tns" userid.

Nessus Configuration for Unix

Commands and Relevant Files

The following section describes the commands and relevant files involved in the Nessus SSL process on a Red Hat Linux system.

Certificate Authority and Nessus Server Certificate

The `/opt/nessus/sbin/nessus-mkcert` command creates the Certificate Authority and generates the server certificate. This command creates the following files:

File Name Created	Purpose	Where to Copy to
/opt/nessus/com/nessus/CA/cacert.pem	This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.	**/opt/nessus/com/nessus/CA** on the initial Nessus server and any additional Nessus servers that need to authenticate using SSL.
/opt/nessus/com/nessus/CA/servercert.pem	This is the public certificate for the Nessus server that is sent in response to a CSR.	**/opt/nessus/com/nessus/CA** on any additional Nessus servers that need to authenticate using SSL.
/opt/nessus/var/nessus/CA/cakey.pem	This is the private key of the Certificate Authority. It may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.	**/opt/nessus/var/nessus/CA** on any additional Nessus servers that need to authenticate using SSL.
/opt/nessus/var/nessus/CA/serverkey.pem	This is the private key of the Nessus server.	**/opt/nessus/var/nessus/CA** on any additional Nessus servers that need to authenticate using SSL.

Nessus Client Keys
The Nessus user, in this case the user ID that SecurityCenter uses to communicate with the Nessus server, is created by the following command:

```
# /opt/nessus/sbin/nessus-mkcert-client
```

This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important to respond "**y**" (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as "user".

The certificate filename will be a concatenation of "**cert_**", the user name you entered and "**.pem**". Additionally, the key filename will be a concatenation of "**key_**", the user name you entered and "**.pem**".

If the user was previously added via the **/opt/nessus/sbin/nessus-adduser** command, you will still need to run this program to register the user. If you have not previously created the user, it is not necessary to also run the **nessus-adduser** command; the user will be created if it does not already exist. The following files are created by this command:

File Name Created	Purpose
/tmp/nessus-xxxxxxxx/cert_{user}.pem	This is the public certificate for the specified user.
/tmp/nessus-xxxxxxxx/key_{user}.pem	This is the private key for the specified user.
/opt/nessus/var/nessus/users/{user}/auth/dname	This is the distinguished name to be associated with this user. The distinguished name consists of a number of fields separated by commas in the following format: "/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}"

Creating and Deploying SSL Authentication for Nessus

An example SSL Certificate configuration for Nessus to SecurityCenter authentication is included below:

In the example described here, SecurityCenter and the Nessus scanner are defined as follows. Your configuration will vary:

SecurityCenter:
IP: 192.168.10.10
OS: Red Hat ES 5

Nessus Scanner:
IP: 192.168.11.30
OS: Red Hat ES 5

Create Keys and User on Nessus Server

Log in to the Nessus scanner and use the **su** command to become the root user. Create the Certificate Authority and Nessus server certificate as follows:

```
# /opt/nessus/sbin/nessus-mkcert
-------------------------------------------------------------------------
                        Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
       Nessus daemon will be able to retrieve this information.

CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]:
Your location (e.g. town) [New York]:
Your organization [Nessus Users United]: Tenable Network Security
This host name [Nessus4_2]:


Congratulations. Your server certificate was properly created.

The following files were created :

. Certification authority :

   Certificate = /opt/nessus//com/nessus/CA/cacert.pem
   Private key = /opt/nessus//var/nessus/CA/cakey.pem

. Nessus Server :
    Certificate = /opt/nessus//com/nessus/CA/servercert.pem
    Private key = /opt/nessus//var/nessus/CA/serverkey.pem
```

Next, create the user ID for the Nessus client, which is SecurityCenter in this case, to log in to the Nessus server with, key and certificate. This is done with the command **/opt/nessus/sbin/nessus-mkcert-client**. If the user does not exist in the Nessus user database, it will be created. If it does exist, it will be registered to the Nessus server and have a distinguished name (dname) associated with it. It is important to respond "**y**" (yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer "**y**" when asked. The following example shows the prompts and typical answers:

```
# /opt/nessus/sbin/nessus-mkcert-client
Do you want to register the users in the Nessus server
as soon as you create their certificates ? [n]: y

------------------------------------------------------------------------
                        Creation Nessus SSL client Certificate
------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [FR]: US
Your state or province name []: MD
Your location (e.g. town) [Paris]: Columbia
Your organization []: Tenable Network Security
Your organizational unit []:
**********
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by
entering a single dot '.'
*********
User #1 name (e.g. Nessus username) []: paul
User paul already exists
Do you want to go on and overwrite the credentials?  [y]: y
Should this user be administrator?  [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Tenable Network Security]:
Organizational unit []:
e-mail []:

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that $login has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
Another client certificate?  [n]: n
Your client certificates are in /tmp/nessus-043c22b5
You will have to copy them by hand
#
```

The certificates created contain the username entered previously, in this case “paul”, and are located in the directory as listed in the example above (e.g., `/tmp/nessus-043c22b5`).

Create the nessuscert.pem Key

In the above specified **`tmp`** directory, the certificate and key files in this example are named “**`cert_paul.pem`**” and “**`key_paul.pem`**”. These files must be concatenated to create **`nessuscert.pem`** as follows:

```
# cd /tmp/nessus-043c22b5
# cat cert_paul.pem key_paul.pem > nessuscert.pem
```

The **nessuscert.pem** file will be used when configuring the Nessus scanner on SecurityCenter. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

Configure Nessus Daemons

To enable certificate authentication on the Nessus server, the **force_pubkey_auth** setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login will be disabled. As the root (or equivalent) user on the Nessus server, run the following command:

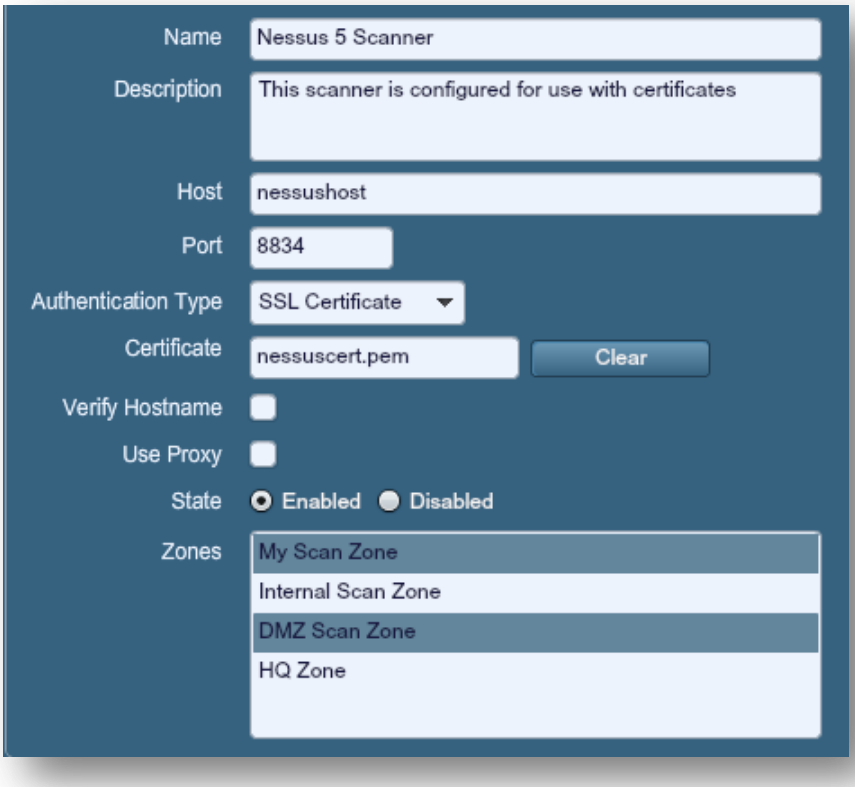
```
# /opt/nessus/sbin/nessus-fix --set force_pubkey_auth=yes
```

Restart the Nessus daemons with the appropriate command for your system. The example here is for Red Hat:

```
# /sbin/service nessusd restart
```

Change the Nessus Mode of Authentication

From the SecurityCenter web UI, go to "**Resources**" and then "**Nessus Scanners**". Change the authentication mode from "Password Based" to "SSL Certificate". During the setup of the Nessus scanner, select the previously created "**nessuscert.pem**" file for the "Certificate" field, then click "**Submit**" to confirm.



Using Custom Certificates

During an upgrade, SecurityCenter will check for the presence of custom SSL certificates. If certificates are found and the owner is not Tenable, any newly generated certificates will be named with a "**.new**" extension and placed in the **/opt/sc4/support/conf** directory to avoid overwriting existing files.

Deploy to other Nessus Scanners

Configure any other Nessus scanners for SecurityCenter use and certificate authentication prior to performing the following tasks.

If you have other Nessus servers that will need to authenticate using the same SSL certificates and user names, simply copy the files to the other servers as follows:

```
# cd /opt/nessus/var/nessus/CA
# scp cakey.pem serverkey.pem root@nessusIP:/opt/nessus/var/nessus/CA
# cd /opt/nessus/com/nessus/CA
# scp cacert.pem servercert.pem root@nessusIP:/opt/nessus/com/nessus/CA
```

You will then need to copy the Nessus user(s) to all the Nessus servers, replacing '`admin`' in the following command with the user's name:

```
# cd /opt/nessus/var/nessus/users
# tar -zcvf - admin | ssh -C root@nessusIP "tar -zxvf - -C
      /opt/nessus/var/nessus/users"
```

Finally, restart the Nessus service on all the Nessus servers with the appropriate command for your system. This example is for Red Hat:

```
# /sbin/service nessusd restart
```

Use the steps from above (**Changing the Nessus Mode of Authentication**) to add the new server(s) to SecurityCenter using certificate-based authentication.

Nessus Configuration for Windows

Commands and Relevant Files

The following section describes the commands and relevant files involved in the Nessus SSL process on a Windows system.

Certificate Authority and Nessus Server Certificate

The **nessus-mkcert.exe** executable located in **C:\Program Files\Tenable\Nessus** creates the Certificate Authority and generates the server certificate. This command creates the following files:

File Name Created	Purpose	Where to Copy to
C:\Program Files\Tenable\Nessus\nessus\CA\cacert.pem	This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.	**C:\Program Files\Tenable\Nessus\nessus\CA** on any additional Nessus servers that need to authenticate using SSL.

C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem	This is the public certificate for the Nessus server that is sent in response to a CSR.	**C:\Program Files\Tenable\Nessus\nessus\CA** on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\cakey.pem	This is the private key of the Certificate Authority. It may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.	**C:\Program Files\Tenable\Nessus\nessus\CA** on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem	This is the private key of the Nessus server.	**C:\Program Files\Tenable\Nessus\nessus\CA** on any additional Nessus servers that need to authenticate using SSL.

Nessus Client Keys

The Nessus user, which in this case is the user ID that SecurityCenter uses to communicate with the Nessus server, is created by the **nessus-mkcert-client.exe** executable located in **C:\Program Files\Tenable\Nessus**.

This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important to respond "**y**" (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as "user".

The certificate filename will be a concatenation of "**cert_**", the user name you entered and "**.pem**". Additionally, the key filename will be a concatenation of "**key_**", the user name you entered and "**.pem**".

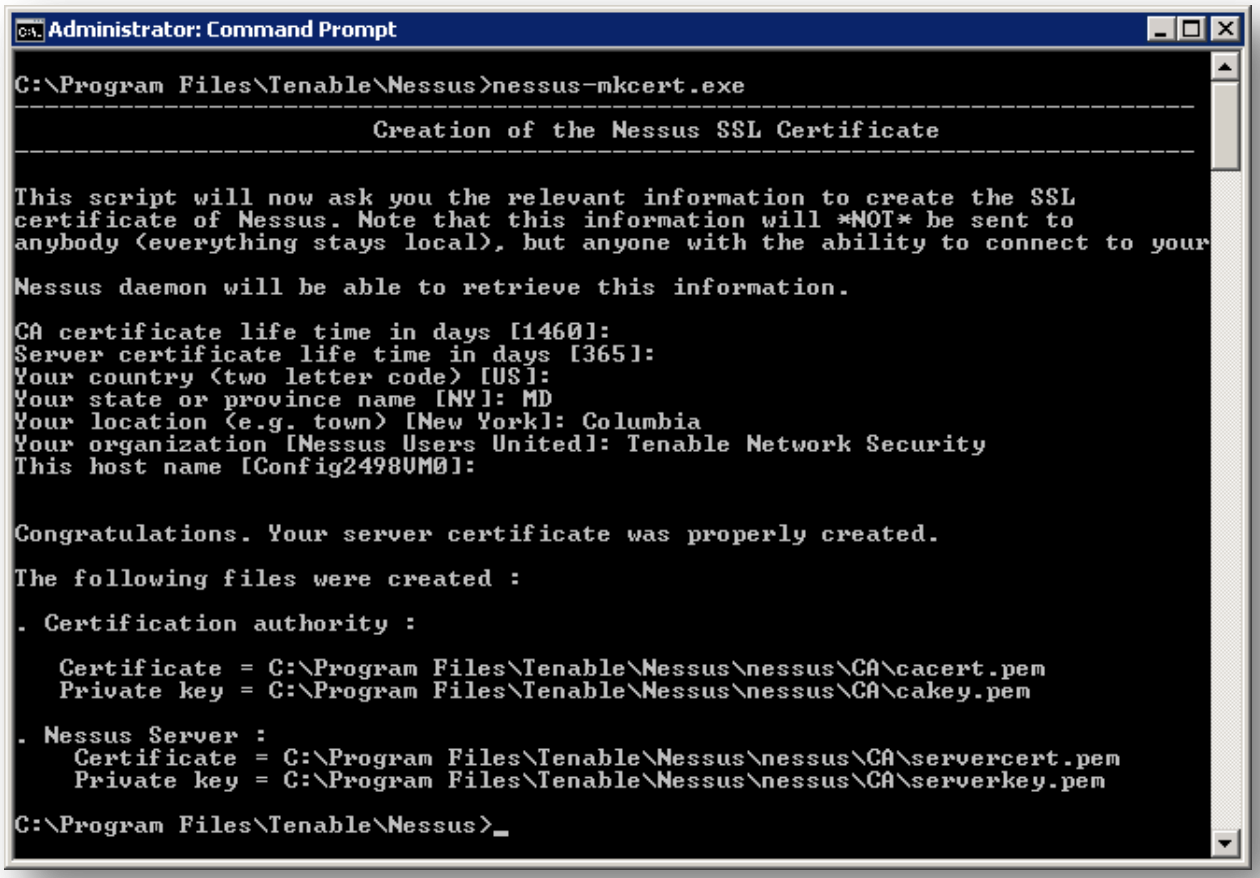
The following files are created by this command:

File Name Created	Purpose
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxxx\cert_<user>.pem	This is the public certificate for the specified user.
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxxx\key_<user>.pem	This is the private key for the specified user.
C:\Program Files\Tenable\Nessus\nessus\users\<user_name>\auth\dname	This is the distinguished name to be associated with this user. The distinguished name consists of a number of fields separated by commas in the following format: "/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}"

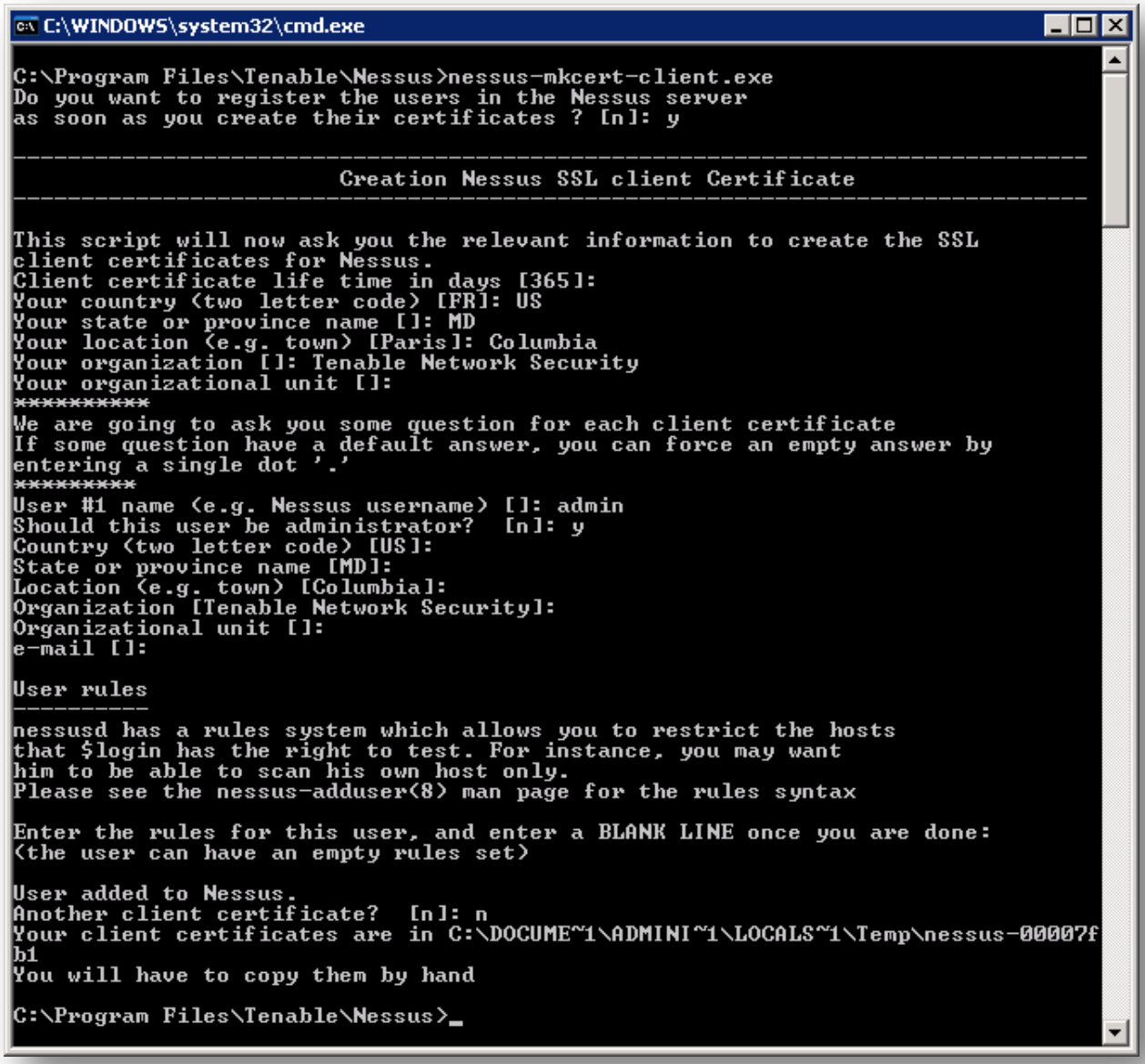
Creating and Deploying SSL Authentication for Nessus

Create Keys and User on Nessus Server

Create the Certificate Authority and Nessus server certificate using the **nessus-mkcert.exe** executable located in **C:\Program Files\Tenable\Nessus** as follows:


Administrator: Command Prompt
C:\Program Files\Tenable\Nessus>nessus-mkcert.exe
Creation of the Nessus SSL Certificate
This script will now ask you the relevant information to create the SSL
certificate of Nessus. Note that this information will *NOT* be sent to
anybody (everything stays local), but anyone with the ability to connect to your
Nessus daemon will be able to retrieve this information.
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]: MD
Your location (e.g. town) [New York]: Columbia
Your organization [Nessus Users United]: Tenable Network Security
This host name [Config2498VM0]:
Congratulations. Your server certificate was properly created.
The following files were created :
. Certification authority :
Certificate = C:\Program Files\Tenable\Nessus\nessus\CA\cacert.pem
Private key = C:\Program Files\Tenable\Nessus\nessus\CA\cakey.pem
. Nessus Server :
Certificate = C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem
Private key = C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem
C:\Program Files\Tenable\Nessus>

Next, create the user ID for the Nessus client, which is SecurityCenter in this case, to log in to the Nessus server with, key and certificate. This is done with the **`nessus-mkcert-client.exe`** executable located in **`C:\Program Files\Tenable\Nessus`**. If the user does not exist in the Nessus user database, it will be created. If it does exist, it will be registered to the Nessus server and have a distinguished name (dname) associated with it. It is important to respond "**y**" (yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer "**y**" when asked. The following example shows the prompts and typical answers:


C:\WINDOWS\system32\cmd.exe
C:\Program Files\Tenable\Nessus>nessus-mkcert-client.exe
Do you want to register the users in the Nessus server
as soon as you create their certificates ? [n]: y
Creation Nessus SSL client Certificate
This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [FR]: US
Your state or province name []: MD
Your location (e.g. town) [Paris]: Columbia
Your organization []: Tenable Network Security
Your organizational unit []:
We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by
entering a single dot '.'
User #1 name (e.g. Nessus username) []: admin
Should this user be administrator? [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Tenable Network Security]:
Organizational unit []:
e-mail []:
User rules
nessusd has a rules system which allows you to restrict the hosts
that $login has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax
Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)
User added to Nessus.
Another client certificate? [n]: n
Your client certificates are in C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nessus-00007fb1
You will have to copy them by hand
C:\Program Files\Tenable\Nessus>

The certificates created contain the username entered previously, in this case “admin”, and are located in the directory as listed in the example screen capture above (e.g., **`C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-00007fb1`**). In the specified directory, the certificate and key files in this example are named “**`cert_admin.pem`**” and “**`key_admin.pem`**”.

Transfer Certificates and Keys to SecurityCenter

Transfer the “**`cert_admin.pem`**” and “**`key_admin.pem`**” files to a desired location on SecurityCenter, change into that directory and concatenate them as follows:

```
# cat cert_admin.pem key_admin.pem > nessuscert.pem
```

The **nessuscert.pem** file will be used when configuring the Nessus scanner on SecurityCenter. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

Configure Nessus Daemons

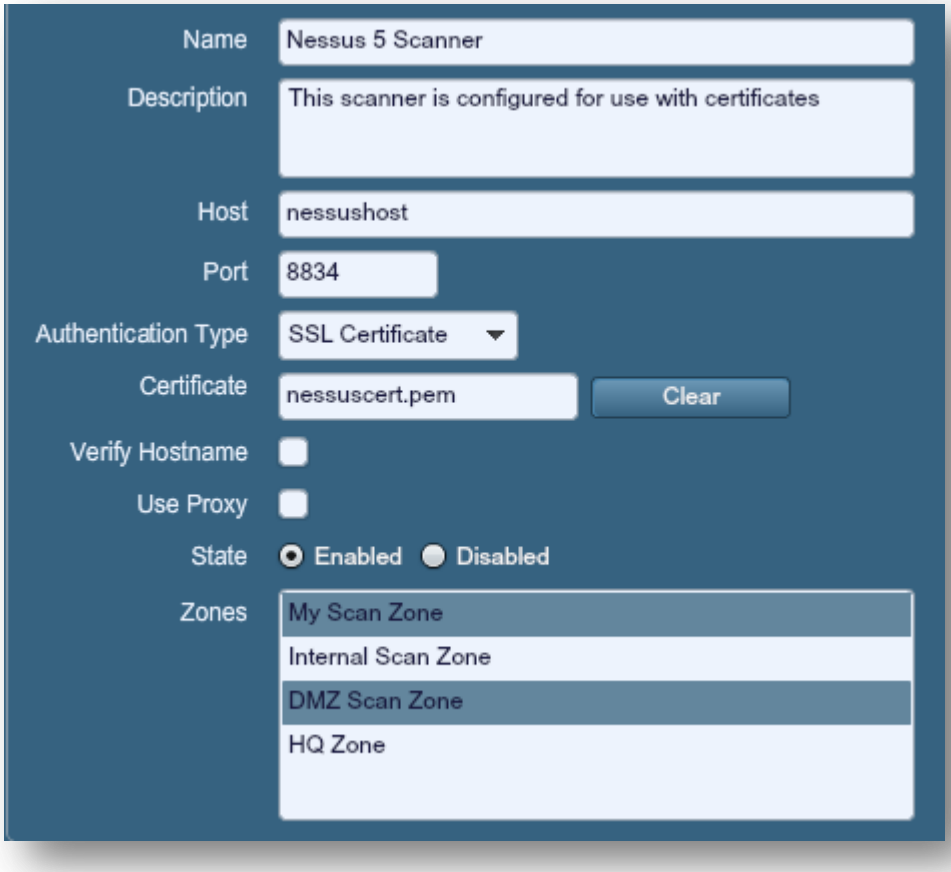
To enable certificate authentication on the Nessus server, the **force_pubkey_auth** setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login will be disabled. As the root (or equivalent) user on the Nessus server, run the following command:

```
C:\Program Files\Tenable\Nessus\nessus-fix --set force_pubkey_auth=yes
```

Open the Nessus Server Manager GUI, click “Stop Nessus Server” and then click “Start Nessus Server”.

Change the Nessus Mode of Authentication

From the SecurityCenter web UI, go to “**Resources**” and then “**Nessus Scanners**”. Change the authentication mode from “Password Based” to “SSL Certificate”. During the setup of the Nessus scanner, select the previously created “**nessuscert.pem**” file for the “Certificate” field, then click “**Submit**” to confirm.



Appendix 4: Using a Custom SSL Certificate

SecurityCenter ships with its own default SSL certificate; however, in many cases it is desirable to obtain a custom SSL certificate for enhanced security.

In the example below, two certificate files were received from the CA: "**host.crt**" and "**host.key**". These file names will vary depending on the CA used.

The custom certificate email address must not be "SecurityCenter@SecurityCenter" or subsequent upgrades will not retain the new certificate.

Use the steps below to upload a custom SSL certificate to your SecurityCenter:

1. Backup the current certificates that are located in the **/opt/sc4/support/conf** directory. These files are named **SecurityCenter.crt** and **SecurityCenter.key**. In the example below, we are placing the files in **/tmp**.

```
# cp /opt/sc4/support/conf/SecurityCenter.crt /tmp/SecurityCenter.crt.bak
# cp /opt/sc4/support/conf/SecurityCenter.key /tmp/SecurityCenter.key.bak
```

2. Copy the new certificates (e.g., **host.crt** and **host.key**) to the **/opt/sc4/support/conf** directory and overwrite the current certificates. If prompted to overwrite, press "y".

```
# cp host.crt /opt/sc4/support/conf/SecurityCenter.crt
# cp host.key /opt/sc4/support/conf/SecurityCenter.key
```

3. Make sure the files have the correct permissions (644) and ownership (tns) as follows:

```
# ls -l /opt/sc4/support/conf/SecurityCenter.crt
-rw-r--r--  1 tns tns  4389 May 15 15:12 SecurityCenter.crt
# ls -l /opt/sc4/support/conf/SecurityCenter.key
-rw-r--r--  1 tns tns   887 May 15 15:12 SecurityCenter.key
```

If an intermediate certificate is required, it must be copied to the system and given the correct permissions (644) and ownership (tns). Additionally, the line in **/opt/sc4/support/conf/vhostssl.conf** that begins with `#SSLCertificateChainFile` must have the "#" removed from the beginning of the line to enable the setting. Modify the path and filename to match the certificate that was uploaded.

4. Restart the SecurityCenter services:

```
# service SecurityCenter restart
```

5. Browse to SecurityCenter using SSL (e.g., https://192.168.1.5). When prompted to confirm the SSL certificate, verify the new certificate details.

Appendix 5: Offline SecurityCenter Plugin Updates

Nessus

1. If not already in place, install a Nessus scanner on the same host as SecurityCenter. It does not need to be started or used though.

2. Run this command and save the challenge string:

   ```
   # /opt/nessus/bin/nessus-fetch --challenge
   ```

3. Go to https://plugins-customers.nessus.org/offline.php.

4. Take the challenge string from Step 2 and your Activation Code, and place those values in the appropriate fields on the web page. Click the “Submit” button.

5. On the next page, copy the link that starts with http://plugins.nessus.org/get.php... and save it as a favorite. Within the saved link change “all-2.0.tar.gz” to “sc-plugins-diff.tar.gz”. This link may be needed for future use. Do not click the link for **`nessus-fetch.rc`** as it is not needed.

6. Go to the favorite you created, this will prompt you to download a file. Download the file; it will be called **`sc-plugins-diff.tar.gz`**.

7. Take the **`sc-plugins-diff.tar.gz`** and save this on the PC where you access your SecurityCenter GUI.

8. Log into the SecurityCenter GUI as admin.

9. Go to Plugins -> Plugins.

10. Click “Upload Plugins” and browse to the saved **`sc-plugins-diff.tar.gz`** file, and then click “Submit”.

11. The plugin update will take a few to several minutes, depending how many Nessus scanners you have attached. A message with the current date for the updated active plugins will appear when the update is finished.

PVS (SecurityCenter 4.2 and greater only)

1. Go to http://downloads.nessus.org/sc-passive.tar.gz and download the archive to a location browseable from SecurityCenter.

2. Log into SecurityCenter and go to “**Plugins**” and then “**Upload**”. Choose the sc-passive.tar.gz file. For type, select “Passive” and then complete the PVS plugin upload.

Appendix 6: Configuring LDAP with Multiple Organizational Units

Tenable's SecurityCenter LDAP configuration does not currently support the direct addition of multiple Organizational Units (OUs) in the LDAP configuration screen. Two deployment options are possible for those with multiple OUs:

Option 1 (Preferred)

Add a container (i.e., Group) only for SecurityCenter users and allow existing Active Directory users to become members of the newly created group. Use the Distinguished Name (DN) of this group as the "Search Base". For example:

```
CN=SecurityCenter,DC=devlab,DC=domain,DC=com
```

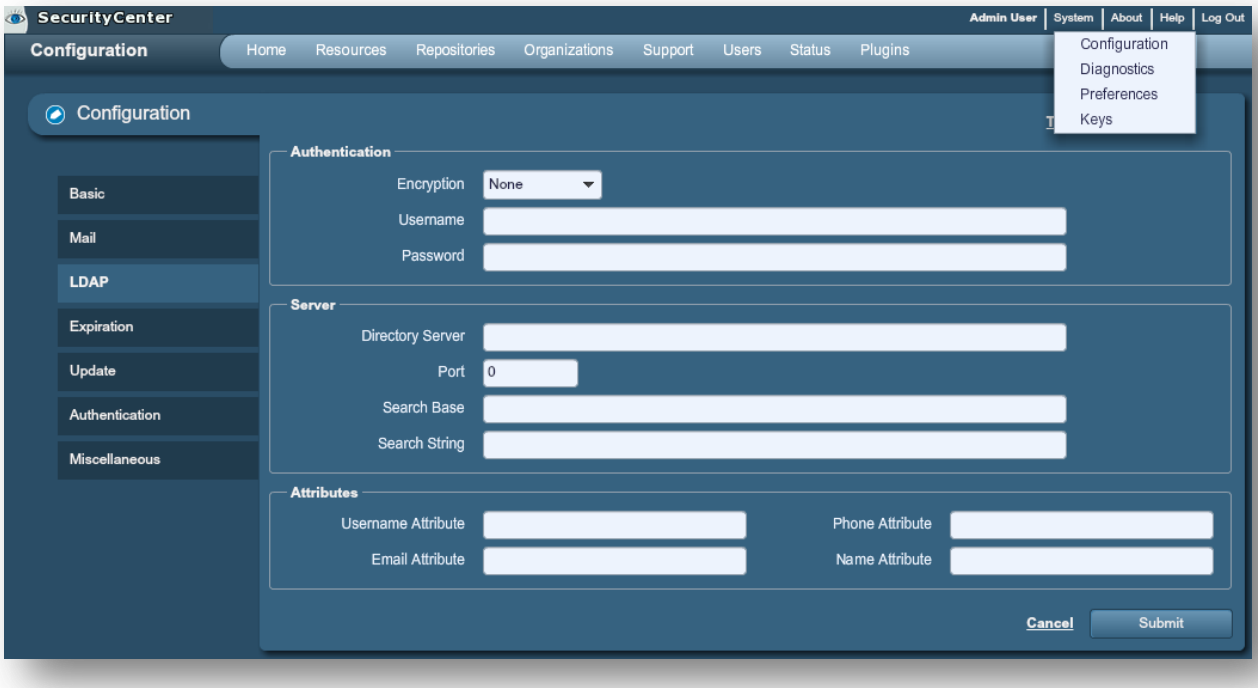
Save the changes and new users who are members of this group will be able to log in. No restart is required.

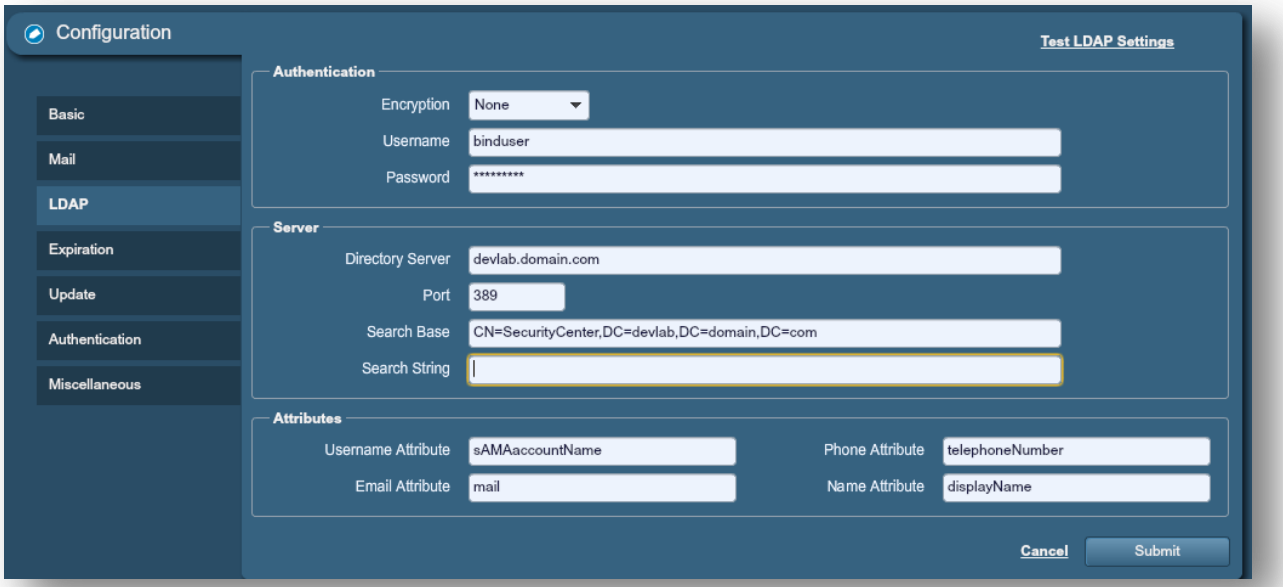
Option 1 Example

Step One:

a. Log in as an admin user.

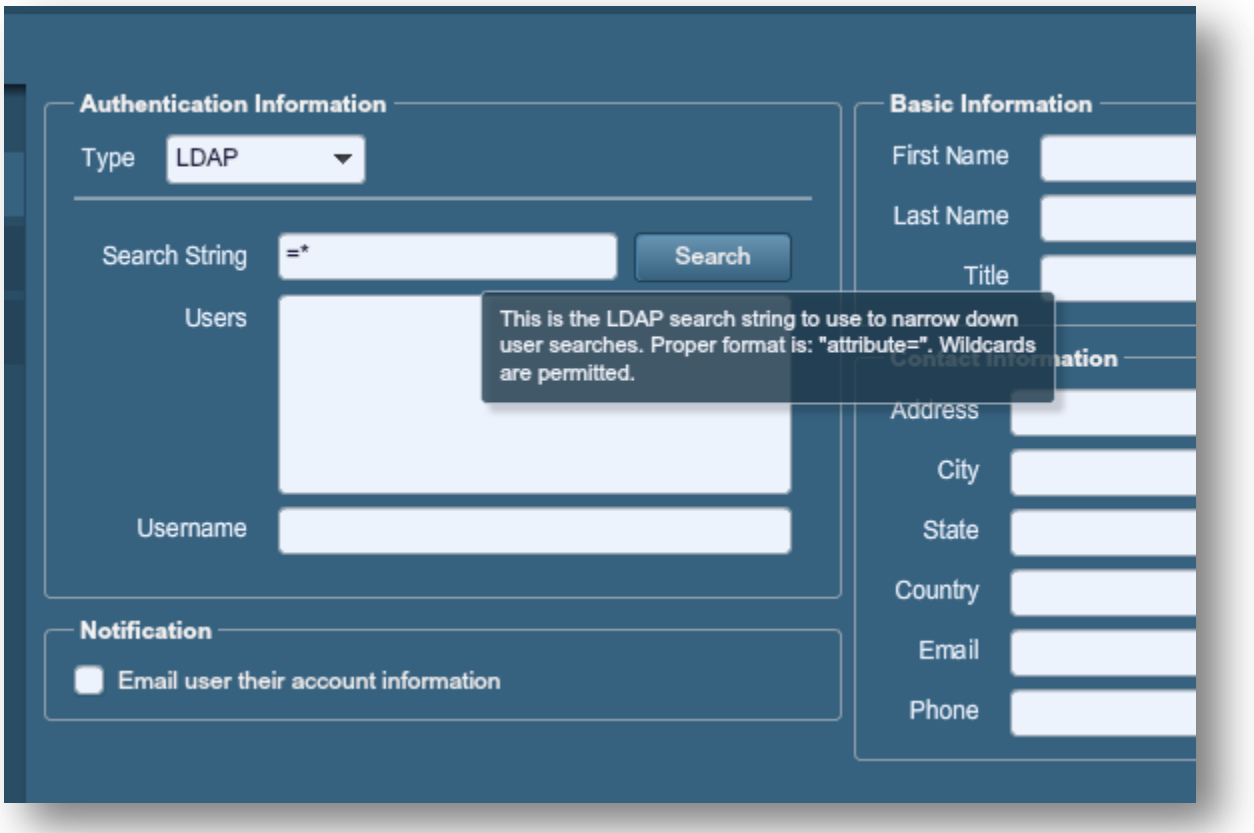
b. Choose System -> Configuration -> LDAP





c. Log out as the admin user and then log in as the organizational user who will be managing the user in question.

d. Create the new user and when entering the LDAP “Search String” enter “=*”:



Option 2

Use a high level “Search Base” in the LDAP configuration. For example:

```
DC=devlab,DC=domain,DC=com
```

The example above could be used along with a “Search String” for global usage. This search string, when used in the configuration, will apply to all LDAP searches.

`memberOf=CN=nested1,OU=cftest1,DC=devlab,DC=domain,DC=com`

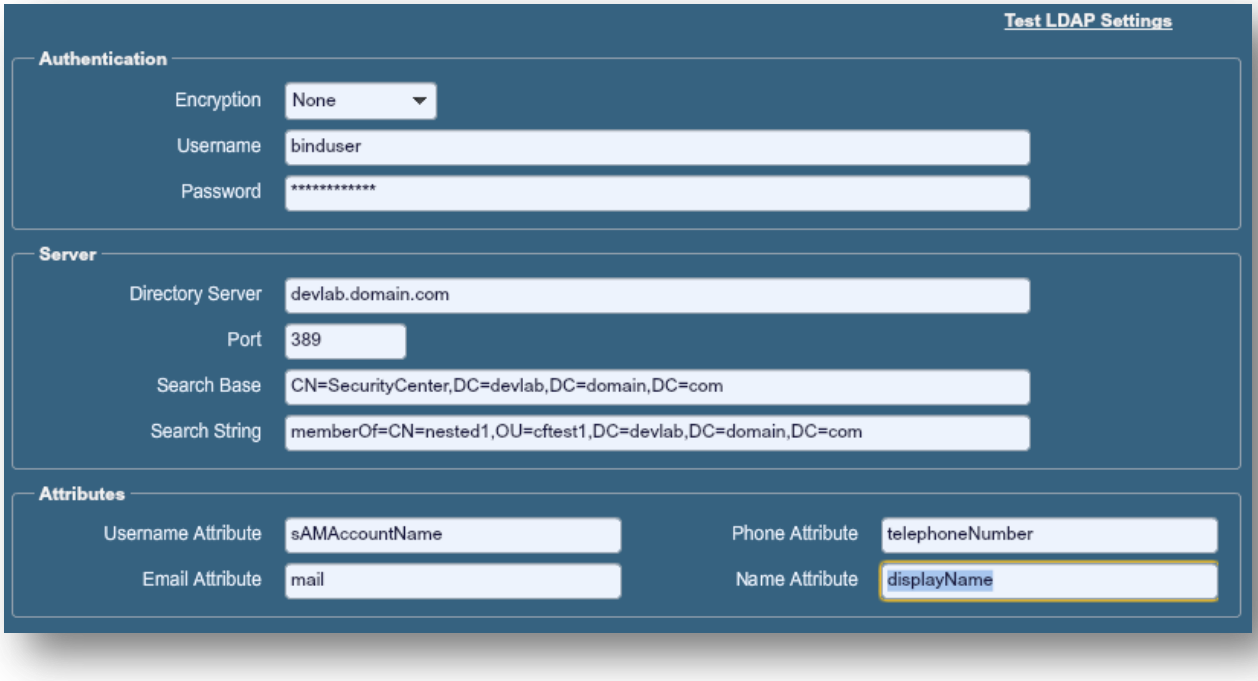
This field is currently limited to 128 characters; we will extend the viewable window and increase the allowed length going forward.

Option 2 Example

Step One:

a. Log in as an admin user.

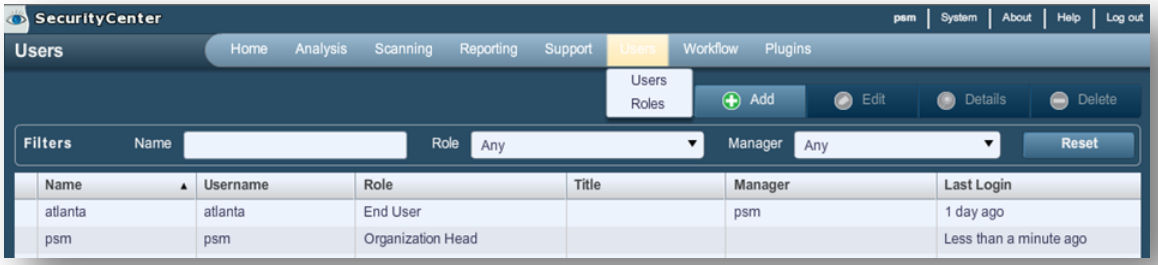
b. Choose System -> Configuration -> LDAP



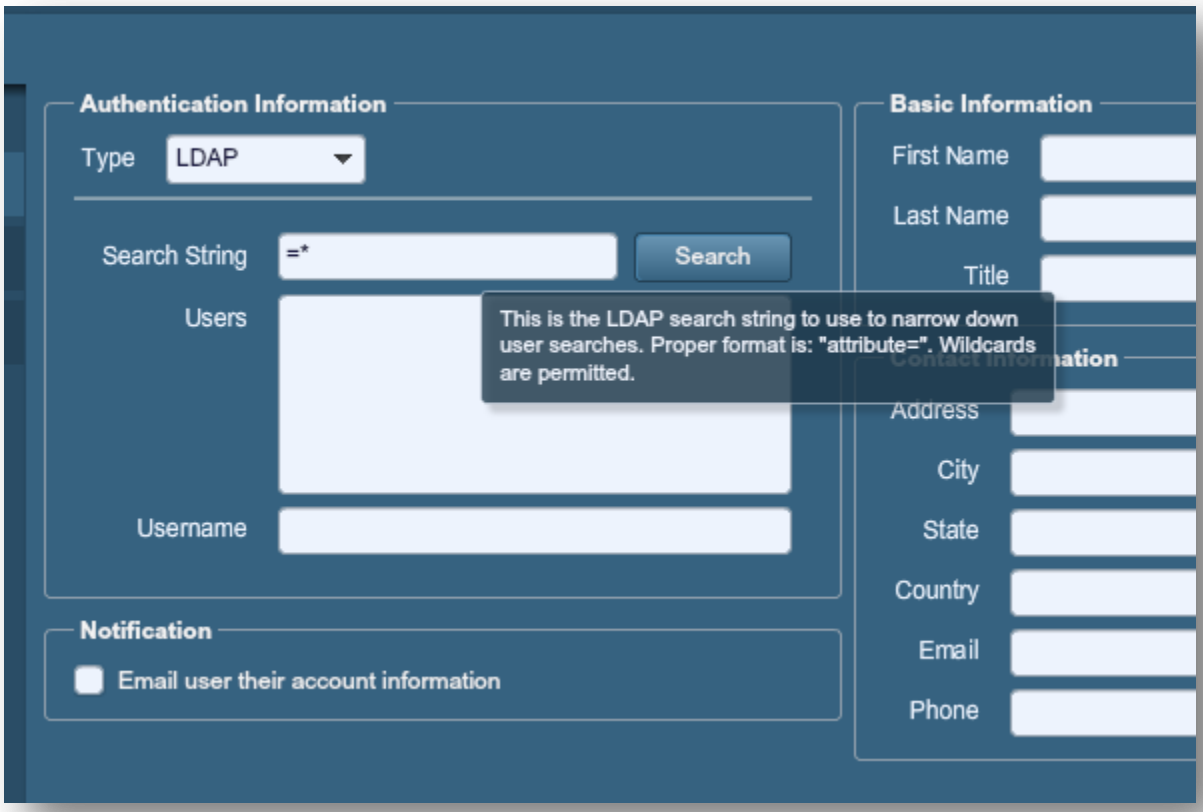
c. Click “Test LDAP Settings” to test configurations.

d. Log out as the admin user and then log in as the organizational user who will be managing the user in question.

e. Create the new user:


SecurityCenter
psm | System | About | Help | Log out
Users
Home Analysis Scanning Reporting Support Users Workflow Plugins
Users
Roles
Add Edit Details Delete
Filters Name Role Any Manager Any Reset
Name Username Role Title Manager Last Login
atlanta atlanta End User psm 1 day ago
psm psm Organization Head Less than a minute ago

Choose LDAP:


Authentication Information
Type LDAP
Search String =*
Search
Users
Username
This is the LDAP search string to use to narrow down user searches. Proper format is: "attribute=". Wildcards are permitted.
Notification
Email user their account information
Basic Information
First Name
Last Name
Title
Address
City
State
Country
Email
Phone

Appendix 7: Configuring SecurityCenter and the LCE for Audit Data Selection

SecurityCenter can be configured in conjunction with the LCE to provide for the selection of audit data to be viewed through the Raw Syslog Data section of SecurityCenter's Analysis Tool.

To accomplish this, SecurityCenter admin logs must be configured to be sent to an LCE server via an LCE client. Per LCE documentation, ensure that an LCE client has initially been installed and configured on the SecurityCenter system and is running:

```
# ps -ef | grep lce_client
root     3156     1   0  11:42  ?     00:00:00     /opt/lce_client/lce_clientd
```

Navigate to the **/opt/lce_client/lce_client.conf** file on the SecurityCenter system and add the following line under the section "`# All files in directories specified with the tail-dir option will be tailed`" to configure the LCE client to send SecurityCenter admin logs to the LCE:

```
tail-dir /opt/sc4/admin/logs/*.log
```

Restart the "**lce_client**" service on the SecurityCenter system:

```
# service lce_client restart
```

Per LCE documentation, ensure that the SecurityCenter's LCE client information has been added to the LCE system's **lce.conf** file in **/opt/lce/daemons/**:

```
# Several formats are supported for specifying client information. These
# are (1) a single IP address, (2) an IP address with a CIDR range,
# (3) optional ranges in the third and fourth octets of the IP address,
# and (4) a range specified by start and end addresses.
# Examples of each follow. In every case, the authentication and sensor
# name defined within the block applies to every client covered by the
# chosen notation.

        client [SecurityCenter IP address] {
        client-auth auth-secret-key [secret key string]
        sensor-name SC_LCE_Sensor
        }
```

An additional line will also need to be added to the **lce.conf** file that will enable the LCE to support multiple plugin matches per log file:

```
#Additional line to provide for multiple matches on LCE plugins
        multiple-matches
```

Please refer to the LCE Administration and User Guide for additional information on "multiple-matches" and multiple plugin matches per log file.

Restart the "**lce**" service on the LCE system:

```
# service lce restart
```

By default, the LCE system comes with a PRM file called "**tenable_sc4_logs.prm**" that contains events that are audited by SecurityCenter. To enable the selection of auditable events from the set of events that are audited by default on SecurityCenter, the **tenable_sc4_logs.prm** file can be copied to a new PRM file, edited, saved, and then searched upon through a filter in the SecurityCenter Analysis Tool's "Raw Syslog Data" selection.

To create and edit the new selection-based PRM file, navigate to **/opt/lce/daemons/plugins** on the LCE system and confirm the existence of the **tenable_sc4_logs.prm** file:

```
# ls -la tenable_sc4_logs.prm
-rwxr-x--- 1 lce lce 17191 Oct 17 14:40 tenable_sc4_logs.prm
```

As a user with permissions to manipulate files in this directory, such as 'root' or 'lce', copy the tenable_sc4_logs.prm file to a file with a similar but new name:

```
# cp tenable_sc4_logs.prm tenable_sc4_audit_logs.prm
```

Open the new file with a text editor to make changes to the new file. The first set of changes will be to create a unique "type:" for each event listed in the new PRM file in order to facilitate searches through SecurityCenter directly against the new PRM file. In the example shown below, the "id=" is given a unique number, the "type:" for the "name=The Security Center had a successful login." event has been changed to "loginfo":

```
id=8272
name=The Security Center had a successful login.
match= -
match=FO
match=|auth|
match=IN
match=|INFO|
match=lo
match=log
match=ce
match=ss
match=Successful login for
regex=Successful login for '([A-Za-z0-9\$\-\_]{1,25})' from ([0-9]+(\.[0-9]+){3})
log=event:SC4-Login user:$1 srcip:$2 type:loginfo
```

Selection or de-selection of events is accomplished through commenting or uncommenting events within the new PRM file. For example, if your organization does not wish to audit SecurityCenter login events, find the "The SecurityCenter had a successful login" section of the new file and add a "#" character to comment out the "id", "name", "match", "regex" and "log" lines for that event:

```
#id=8272
#name=The Security Center had a successful login.
#match= -
#match=FO
#match=|auth|
#match=IN
#match=|INFO|
#match=lo
#match=log
#match=ce
#match=ss
#match=Successful login for
#regex=Successful login for '([A-Za-z0-9\$\-\_]{1,25})' from ([0-9]+(\.[0-9]+){3})
#log=event:SC4-Login user:$1 srcip:$2 type:loginfo
```

When edits are completed, save the new PRM file to its current location. Ensure the file is owned by the lce user and lce group with the correct permissions by running the following commands:

```
# chmod 750 tenable_sc4_audit_logs.prm
# chown lce:lce tenable_sc4_audit_logs.prm
```

The original PRM may be disabled by adding the name of the file to the **/opt/lce/admin/disabled-prms.txt** file. See the section Excluding PRM Files in the LCE documentation.

After ownership and permissions are set, restart the “lce” service:

```
# service lce restart
```

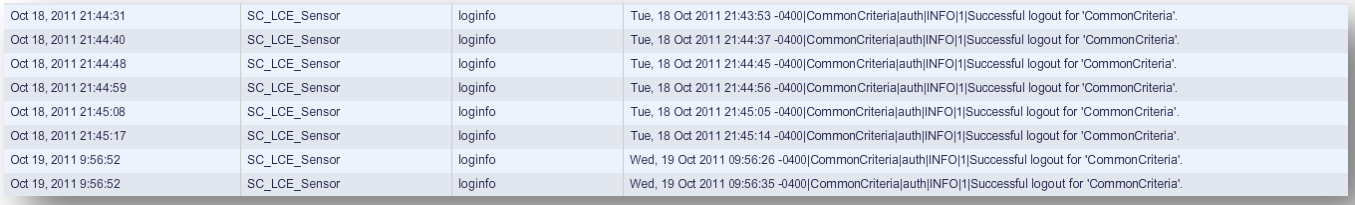
To view the current selection and/or de-selection of auditable events through the new PRM file, log into SecurityCenter as an Organization Head (you may wish to create a new unique Organization Head account specifically for this function).

Note that because SecurityCenter administrator accounts do not have access to log data under “Analysis > Events” in SecurityCenter, an Organization Head account is best suited to perform this function. It is recommended to create a new Organization Head account that is only accessible by SecurityCenter administrators to view the logs in their selected form.

Once logged in, select “**Analysis** > **Events**”. Under the Analysis Tool, select “**Raw Syslog Data**” from the drop-down menu. Note that the filter conditions will need to be applied before the viewability of events in the new PRM file are applied to the overall audit log data set.

To specifically target the SecurityCenter’s LCE client data, select a filter of “Type = [custom_type_name]”, where [custom_type_name] is the unique event type (`loginfo` in the example above) created for the customized PRM file (**`tenable_sc4_audit_logs.prm`** in the example above):

In the example screen capture below, only logout information is displayed for SecurityCenter users because the login section of the newly-created PRM file has been commented out:



Oct 18, 2011 21:44:31	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:43:53 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 18, 2011 21:44:40	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:44:37 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 18, 2011 21:44:48	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:44:45 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 18, 2011 21:44:59	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:44:56 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 18, 2011 21:45:08	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:45:05 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 18, 2011 21:45:17	SC_LCE_Sensor	loginfo	Tue, 18 Oct 2011 21:45:14 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 19, 2011 9:56:52	SC_LCE_Sensor	loginfo	Wed, 19 Oct 2011 09:56:26 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.
Oct 19, 2011 9:56:52	SC_LCE_Sensor	loginfo	Wed, 19 Oct 2011 09:56:35 -0400|CommonCriteria|auth|INFO|1|Successful logout for 'CommonCriteria'.

Other sections of the custom PRM file can be commented or uncommented by an authorized system administrator to allow for selection of audited events per your organization’s logging requirements. Each change to the custom PRM file will require a restart of the LCE services.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com

Copyright © 2013. Tenable Network Security, Inc. All rights reserved. Tenable Network Security and Nessus are registered trademarks of Tenable Network Security, Inc.